# Privacy in DeFi: Challenges and Constructions

ZK Summit 7

Guillermo Angeris

April 21, 2022

# Outline

Overview and a warning

Definitions

The interesting stuff

Conclusion

# This talk

- Mostly a high level talk about ‘privacy’

# This talk

- Mostly a high level talk about ‘privacy’
- What is it?
- How do we define it?

# This talk

- Mostly a high level talk about ‘privacy’
- What is it?
- How do we define it?
- Focus on *clean* definitions/constructions/ideas

# A warning

- Many will already know this!

# A warning

- Many will already know this!
- Likely in a very different way

# A warning

- Many will already know this!
- Likely in a very different way
- Probably in more generality than needed!

# Outline

Overview and a warning

Definitions

The interesting stuff

Conclusion

# A mechanism

- Start with some *disclosure mechanism*

# A mechanism

- Start with some *disclosure mechanism*
- This is a function $T : \mathcal{A} \to \mathcal{S}$
- Maps (private) action $a \in \mathcal{A}$ to a (public) state $s \in \mathcal{S}$

# A mechanism

- Start with some *disclosure mechanism*
- This is a function $T : \mathcal{A} \to \mathcal{S}$
- Maps (private) action $a \in \mathcal{A}$ to a (public) state $s \in \mathcal{S}$
- $T$ can be anything!
  - CFMM taking trade $a$, reporting post-trade price $s$
  - Loan borrowed for amount $a$, reporting new interest $s$

## An adversary

- We have some protocol with disclosure mechanism $T$
- Alice performs some action $a$, revealing public information $s = T(a)$
- Eve wants to reconstruct action $a$ given public info $s$

# An adversary

- We have some protocol with disclosure mechanism $T$
- Alice performs some action $a$, revealing public information $s = T(a)$
- Eve wants to reconstruct action $a$ given public info $s$
- The big question: what can Eve learn from public data $s$?
- (We will not directly deal with history, anonymity, *etc.*)

# Some observations

- Eve can look at the *preimage* of $s$

$$T^{-1}(s) = \{a' \in \mathcal{A} \mid T(a') = s\}$$

## Some observations

- Eve can look at the *preimage* of $s$

$$T^{-1}(s) = \{a' \in \mathcal{A} \mid T(a') = s\}$$

- $T^{-1}(s)$ is nonempty
- The 'larger' $T^{-1}(s)$ is, the 'harder' finding $a$ is

# Some observations

- Eve can look at the *preimage* of $s$

$$T^{-1}(s) = \{a' \in \mathcal{A} \mid T(a') = s\}$$

- $T^{-1}(s)$ is nonempty
- The ‘larger’ $T^{-1}(s)$ is, the ‘harder’ finding $a$ is
- (we will quantify this soon)

# An example

- In many cases the set $T^{-1}(s)$ is very small

## An example

- In many cases the set $T^{-1}(s)$ is very small
- *e.g.*, in CFMMs, $T^{-1}(s)$ is a singleton! [AEC'21]

# An example

- In many cases the set $T^{-1}(s)$ is very small
- *e.g.*, in CFMMs, $T^{-1}(s)$ is a singleton! [AEC'21]
- A question we will pose: what can we do in these cases?

## A final definition

- Before we get there!
- There is some ‘measure’ of ‘size’ of a set, $\mu$

# A final definition

- Before we get there!
- There is some 'measure' of 'size' of a set, $\mu$
- We will only require one property of $\mu$:

$$\mu(A) \leq \mu(B) \quad \text{if} \quad A \subseteq B$$

# A final definition

- Before we get there!
- There is some 'measure' of 'size' of a set, $\mu$
- We will only require one property of $\mu$:

$$\mu(A) \leq \mu(B) \quad \text{if} \quad A \subseteq B$$

- (Sorry measure theorists...)

# Examples

- Silly measure, $\mu(A) = 0$

# Examples

- Silly measure, $\mu(A) = 0$
- Entropy (uniform), $\mu(A) = \log |A|$

# Examples

- Silly measure, $\mu(A) = 0$
- Entropy (uniform), $\mu(A) = \log|A|$
- Probability, $\mu(A) = \textbf{Prob}(a \in A)$

## Examples

- Silly measure, $\mu(A) = 0$
- Entropy (uniform), $\mu(A) = \log |A|$
- Probability, $\mu(A) = \textbf{Prob}(a \in A)$
- Any number of other possibilities!

# Talk about size

- We can now make some sense of 'size'/'privacy'
- Define the *privacy* of disclosed public info $s$ as

$$\mu(T^{-1}(s))$$

# Talk about size

- We can now make some sense of 'size'/'privacy'
- Define the *privacy* of disclosed public info $s$ as

$$\mu(T^{-1}(s))$$

- A mechanism is relatively 'private' under $\mu$ if

$$\inf_s \mu(T^{-1}(s))$$

  is large (what 'large' means depends on $\mu$)

# Outline

Overview and a warning

Definitions

The interesting stuff

Conclusion

# Framework

- Framework, definitions, ideas are very general

# Framework

- Framework, definitions, ideas are very general
- Let's do stuff with them!

# What does Alice need?

- Alice needs to make sure that $T^{-1}(s)$ is large for her action $a$
- From before: measure 'size' by $\mu(T^{-1}(s))$

## What does Alice need?

- Alice needs to make sure that $T^{-1}(s)$ is large for her action $a$
- From before: measure 'size' by $\mu(T^{-1}(s))$
- Clearly, worst case is $\mu(T^{-1}(s)) = \mu(\{a\})$
- (Common in many DeFi applications)
- Can we improve this?

# Batching

- Possible to *batch* actions among Alice, Bob, *etc.*
- If $\bar{a} = \bigoplus_j a_j$ is a 'batching' operator
- Then recovering $a_i$ is (probably) hard!
- Why?

## Batching (continued)

- If there exists a 0-action such that

$$0 \oplus a = a \oplus 0 = a$$

- Many ways of getting the same batched action $\bar{a}$!
- Set of possibilities for player $i$ is

$$P(\bar{a}) = \left\{ a_i \;\middle|\; \bar{a} = \bigoplus_j a_j \right\} \supseteq \{\bar{a}\}.$$

- If $P(\bar{a})$ is always large for any $\bar{a}$ then we have privacy under $\mu$!

# Batching (continued)

- 'Proof': Let $a_1, \ldots, a_n$ be $n$ actions by $n$ players, Alice performs action $a_i$, and protocol aggregates $\bar{a} = \bigoplus_j a_j$, revealing $s = T(\bar{a})$

## Batching (continued)

- 'Proof': Let $a_1, \ldots, a_n$ be $n$ actions by $n$ players, Alice performs action $a_i$, and protocol aggregates $\bar{a} = \bigoplus_j a_j$, revealing $s = T(\bar{a})$
- Define $P(A) = \bigcup_{y \in A} P(y)$
- Possible set of actions Alice could've taken: $P(T^{-1}(s))$, so

$$\mu(P(T^{-1}(s))) \geq \mu(P(a_i))$$

## Batching (continued)

- 'Proof': Let $a_1, \ldots, a_n$ be $n$ actions by $n$ players, Alice performs action $a_i$, and protocol aggregates $\bar{a} = \bigoplus_j a_j$, revealing $s = T(\bar{a})$
- Define $P(A) = \bigcup_{y \in A} P(y)$
- Possible set of actions Alice could've taken: $P(T^{-1}(s))$, so

$$\mu(P(T^{-1}(s))) \geq \mu(P(a_i))$$

- Implies protocol is also 'private' under $\mu$ as

$$\inf_s \mu(P(T^{-1}(s))) \geq \inf_a \mu(P(a))$$

Can derive a slightly stronger version: $(\ldots) \geq \inf_s \sup_{a \in T^{-1}(s)} \mu(P(a))$

# Batching discussion

- Batching never hurts! (Privacy, that is)
- With many players and reasonable assumptions can be very beneficial
- But (a) means you have to define a batching operator
  (not always easy!)
- And (b) UX of batched protocol can be very different

# Randomness

- Another possibility is to add randomness!
- Benefit of not needing other parties
- Allows a user to potentially ‘control’ privacy tradeoff
- Harder to achieve in practice

## Randomness (continued)

- We will write $f_w : \mathcal{A} \to \mathcal{A}$ where $w \sim \mathcal{W}$ is a uniform r.v.
- Alice performs action $a$, mechanism takes $f_w(a)$, releases $s = T(f_w(a))$
- To succeed, Eve has to find $a \in f_w^{-1}(T^{-1}(s))$, but does not know $w$!

## Randomness (continued)

- The uniformity over $\mathcal{W}$ is very useful! (We can extend this)
- Eve 'essentially' (probabilistically) has to decide between

$$\bigcup_{w \in \mathcal{W}} f_w^{-1}(T^{-1}(s))$$

  things
- Given Alice performed $a$ and global info $s$ was released:

$$\mu\left(\bigcup_{w \in \mathcal{W}} f_w^{-1}(T^{-1}(s))\right) \geq \mu\left(\bigcup_{w \in \mathcal{W}} f_w^{-1}(a)\right)$$

## Randomness (continued)

- Can be generalized (and refined):

$$\inf_s \mu\left(\bigcup_{w\in\mathcal{W}} f_w^{-1}(T^{-1}(s))\right) \geq \inf_s \sup_{a\in T^{-1}(s)} \mu\left(\bigcup_{w\in\mathcal{W}} f_w^{-1}(a)\right)$$

- Unfortunately, adversarial power is not really clear in this probabilistic model

- Can be made very explicit in the case where $\mu$ is entropy, gives strong guarantees

## Randomness (continued)

- Can be generalized (and refined):

$$\inf_s \mu\left(\bigcup_{w\in\mathcal{W}} f_w^{-1}(T^{-1}(s))\right) \geq \inf_s \sup_{a\in T^{-1}(s)} \mu\left(\bigcup_{w\in\mathcal{W}} f_w^{-1}(a)\right)$$

- Unfortunately, adversarial power is not really clear in this probabilistic model
- Can be made very explicit in the case where $\mu$ is entropy, gives strong guarantees
- (This is just differential privacy...)

## Outline

Overview and a warning

Definitions

The interesting stuff

Conclusion

# Conclusion

- Simple framework can be used to reason about ‘privacy’
- Can include a number of important cases, depending on guarantees required
- At the end of the day, privacy is about making preimages large!