Mo-nero, Mo-problems

Defending Monero against temporal analysis

Shashvat Srivastava and Henry Heffan

Outline

1. Introduce Monero
2. Problems with current implementation
3. Our mitigations

Introduction

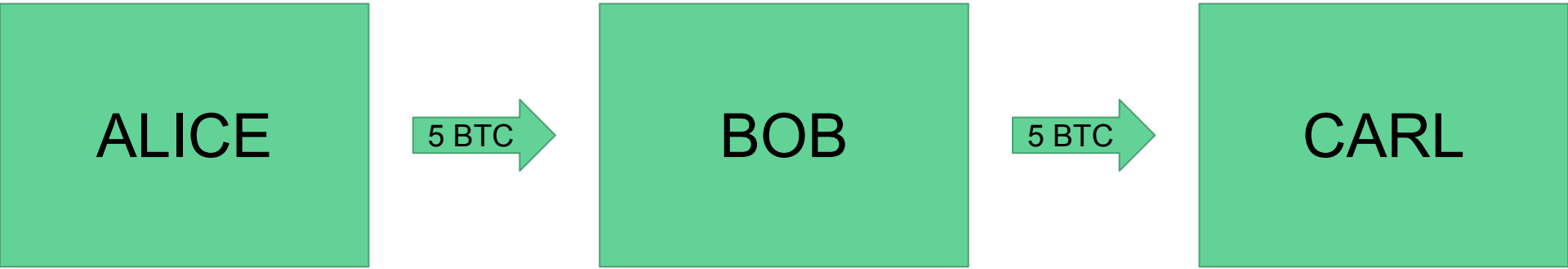
What is Monero?

- Open-source cryptocurrency, like Bitcoin
- Heavy focus on anonymity to hide:
  - Sender
  - Receiver
  - Amount of a transaction

What is a cryptocurrency?

- Cryptocurrencies are a form of digital currency.
- They use encryption to guarantee that currency can only be spent by the proper owner, and that currency can’t be duplicated.
- There are no central authorities in most cryptocurrencies, including Monero.

Bitcoin: the First Cryptocurrency



Bitcoin: Lack of Privacy

PCWorld
FROM IDG

SUBSCRIBE

NEWS | REVIEWS | HOW-TO | VIDEO | BUSINESS | LAPTOPS | TABLETS | PHONES | HARDWARE | SECURITY | SOFTWARE | GADGETS

Privacy | Encryption | Antivirus

Home / Security

NEWS

Bitcoin offers privacy—as long as you don't cash out or spend it

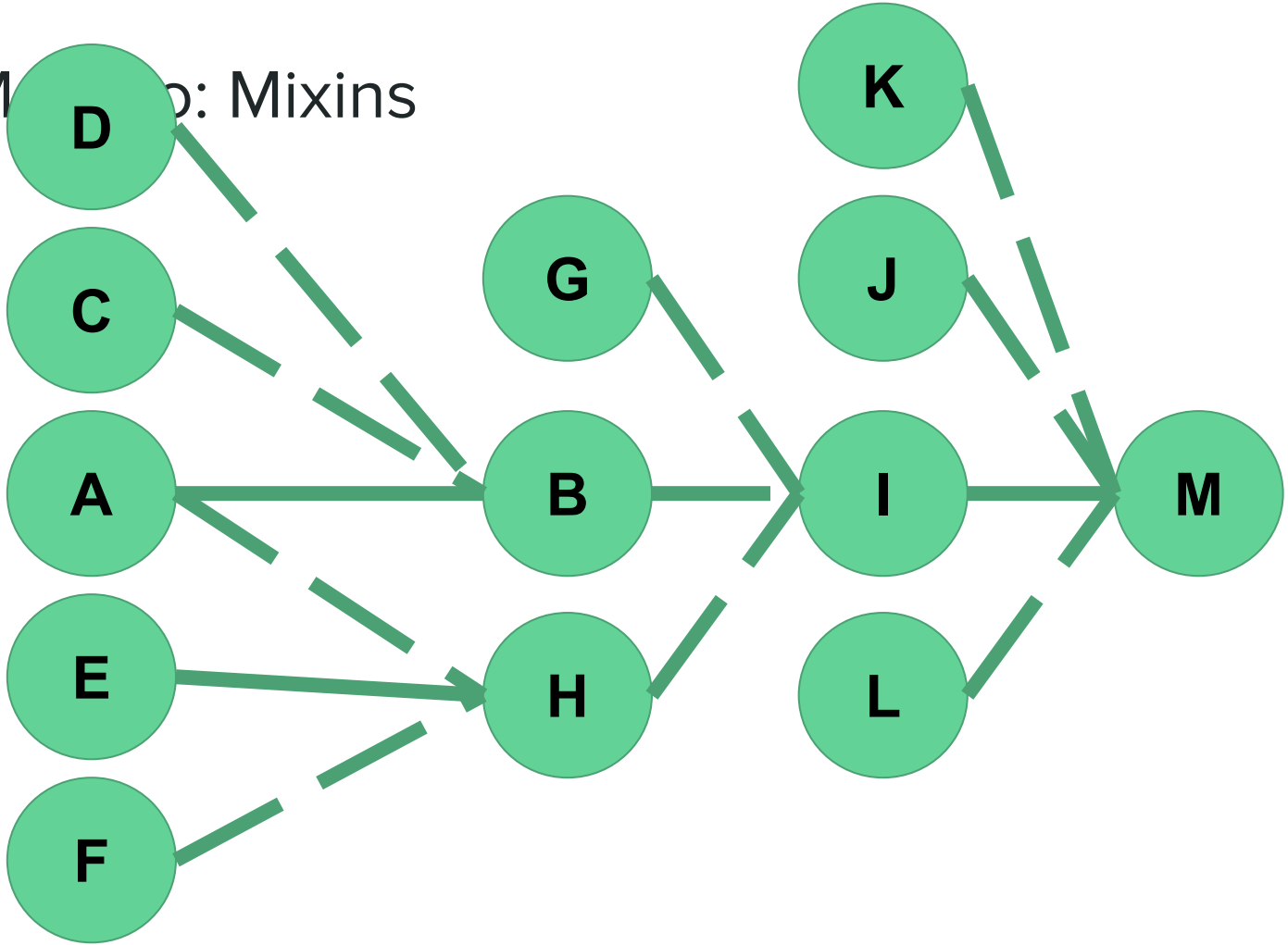
By Jeremy Kirk

Australia Correspondent, IDG News Service | AUG 28, 2013 7:37 AM PT

Monero: Stealth Addresses

Monero: Confidential Transactions

M o: Mixins



So, what is left to be done?

As it turns out, not all of these features are flawless...

Strengths and Weaknesses

- Confidential transactions **work**
- Stealth addresses **work**
- Mixins ... *kinda* work?

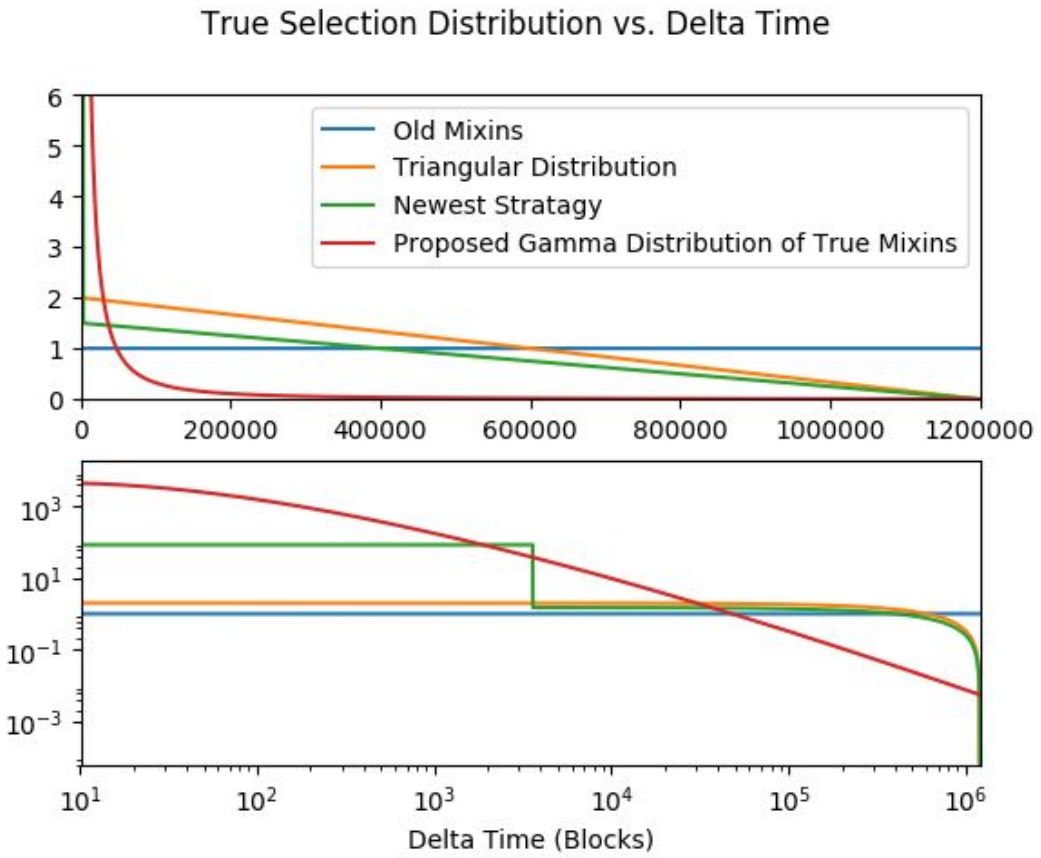
A Measure of Anonymity

- We use guessing entropy as a measure of anonymity.
- We must have an mathematical measure of anonymity in order to analyze our defensive techniques. The below function is the equation for **Guessing Entropy.**
- We define the **Effective Unlikability Set** to be 2 times the Guessing entropy plus 1

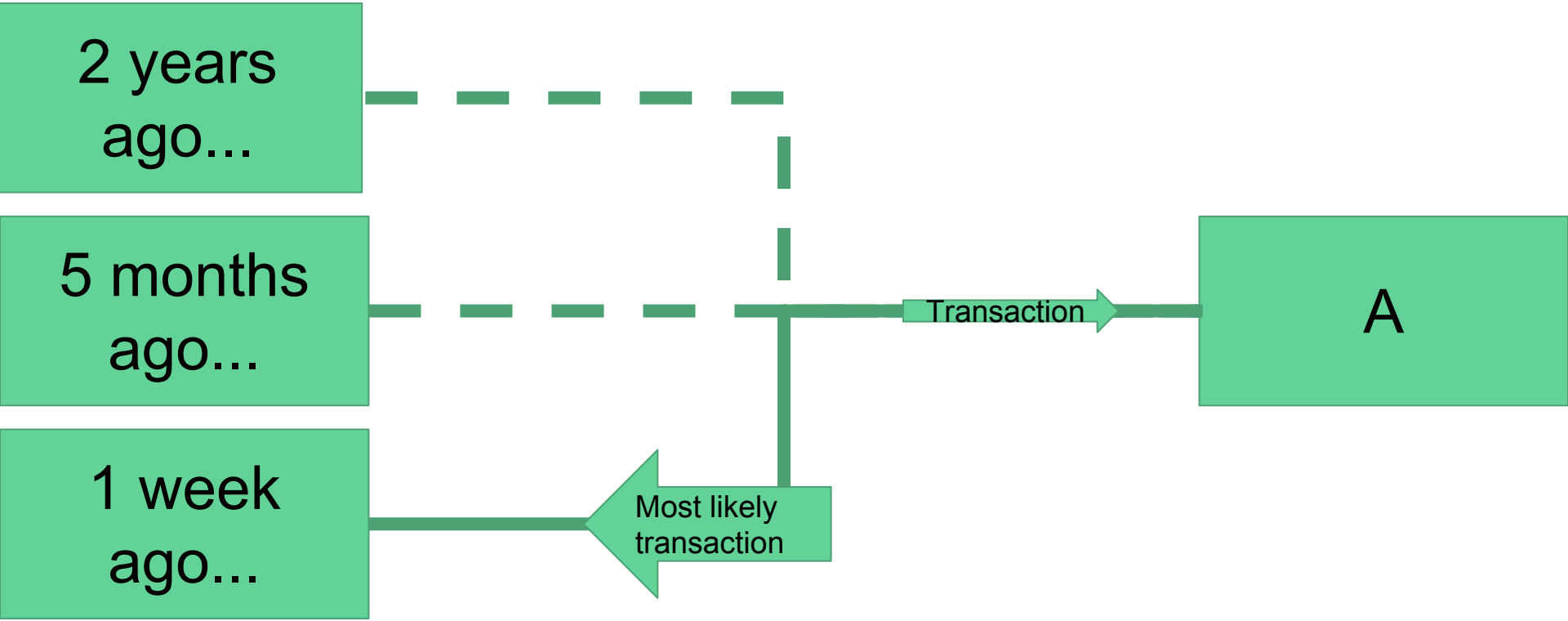
$$A = \sum_{0 \leq i \leq n} i p_i, \;\; p_0 \geq p_1 \geq \cdots \geq p_n$$

Temporal Analysis

- Utilizes the difference between the true output distribution and the mixin selection distribution.
- To the left:
  - a graph of the distributions Monero has used for mixins
  - a recently proposed distribution for the selection of True Mixins in Monero
  - Same graph with log scale



Monero: Temporal Analysis

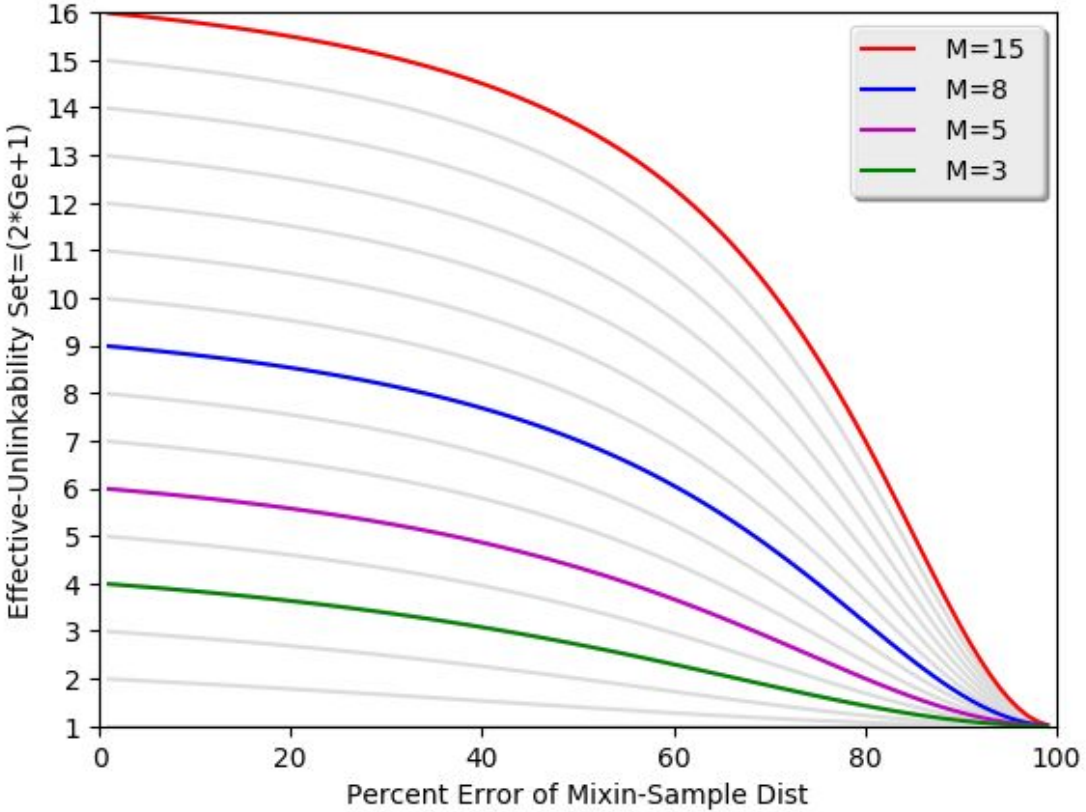


Worst Cases Temporal Attack Anonymity

- If there is a difference in the true output selection distribution and the mixin selection distribution, an attacker has an advantage in guessing what the true output is.
- If we let the maximum error above and below the mixin selection distribution be p, then, if a user select the worst possible mixin

$$A_{min}(n) = \frac{\frac{1}{2}n(n+1)}{\frac{1}{(1-p)^2} + n}$$

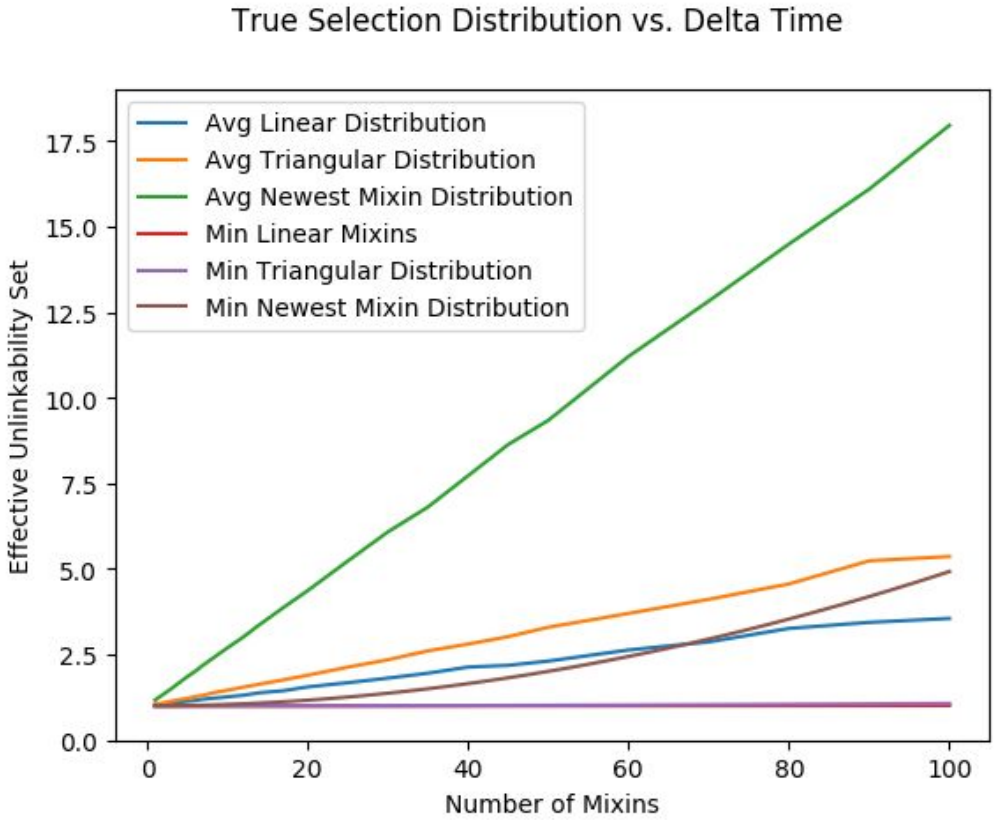
Distribution Based Attack, Effectiveness



Improved Distribution: Monero Now

- As shown by the graph on the previous slide, even a distribution that is mediocre, and therefore somewhat off, still provides significant Anonymity.
- The current problems are only due to the huge discrepancies in selection of mixins and true spends.
    - The maximum ratio between selection of true outputs and mixins is that of 10 blocks ago, which is 53.12. The minimum ration is that of 754002 blocks ago, which is 0.02148.
    - This give an effective percent error of 99.77%.

Anonymity vs. number of mixins currently in Monero



Improved Distribution: Advantages/Disadvantages

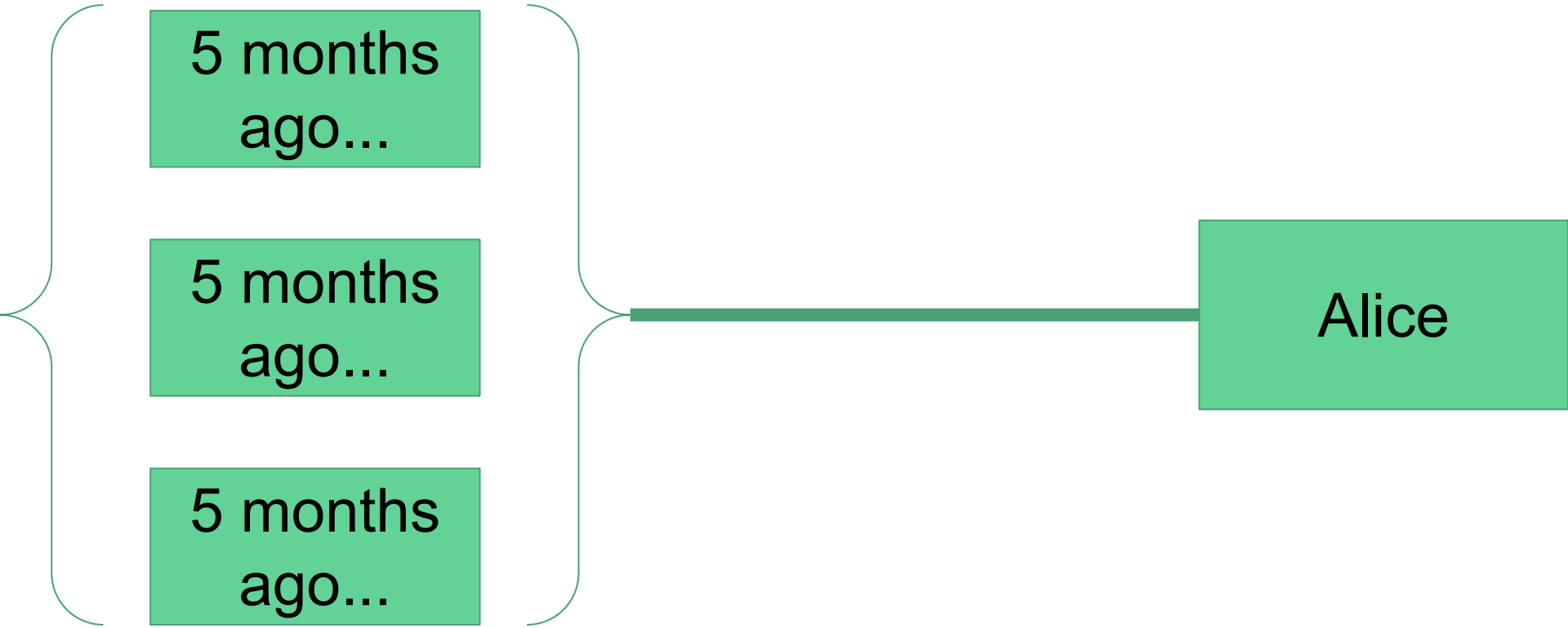
- It will mitigate the effects of temporal analysis
- The distribution can change over time.
- It is impossible to prove that one has the correct distribution. An attacker may come up with a better model of the true spend distribution.
- If the distribution is broken, the true output will be revealed (there is no backup).

Defending Monero

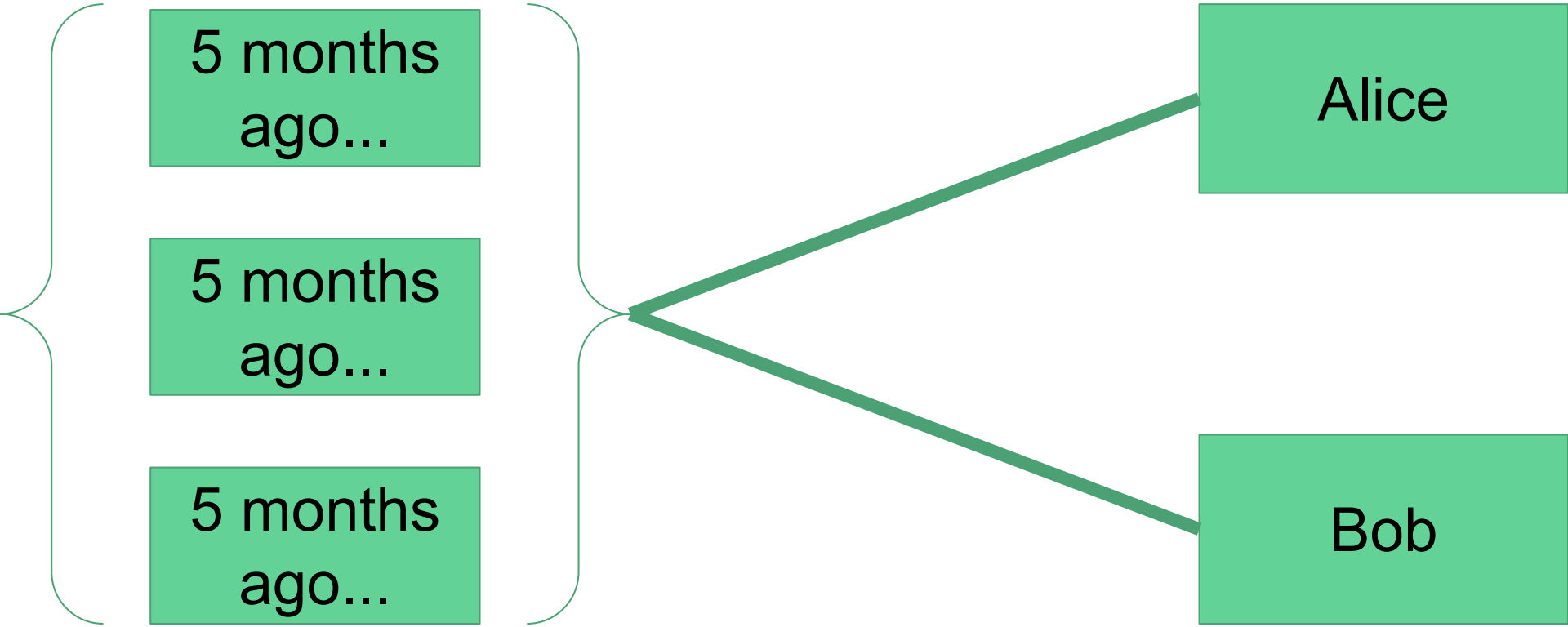
Mixin bins

- Temporal Analysis works by taking advantage of differences in creation time
- However, if all of the mixins were created at the same time...
  - When a node is created, it is assigned to a mixin bin
  - When it creates a transaction, it mixes in ALL other nodes in the mixin bin
  - Every node in the bin mixes in every other node in the bin
  - Temporal analysis fails as every node has the same creation time
- Furthermore, techniques from our first defense can be combined with this defense to allow you to mix in *multiple* bins at the same time

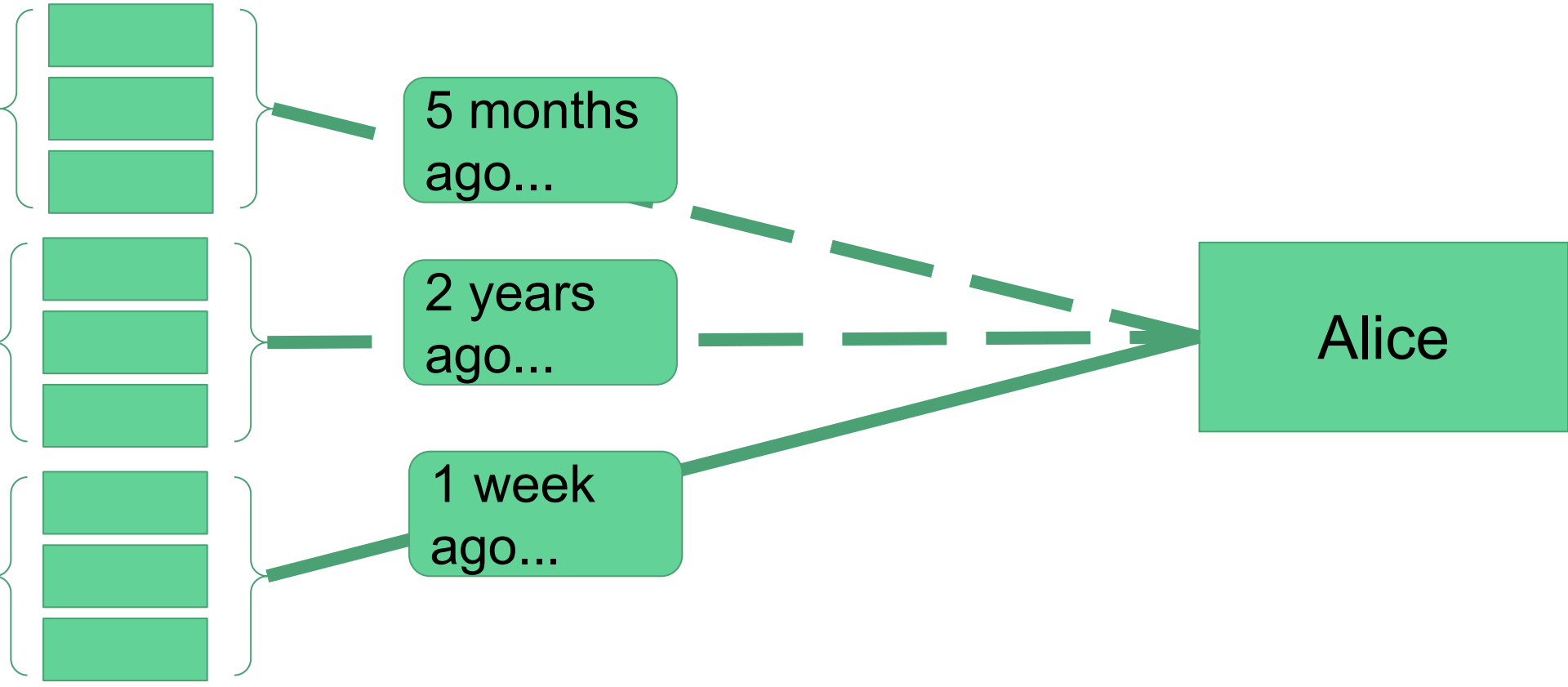
Monero: Singular Mixin Bins



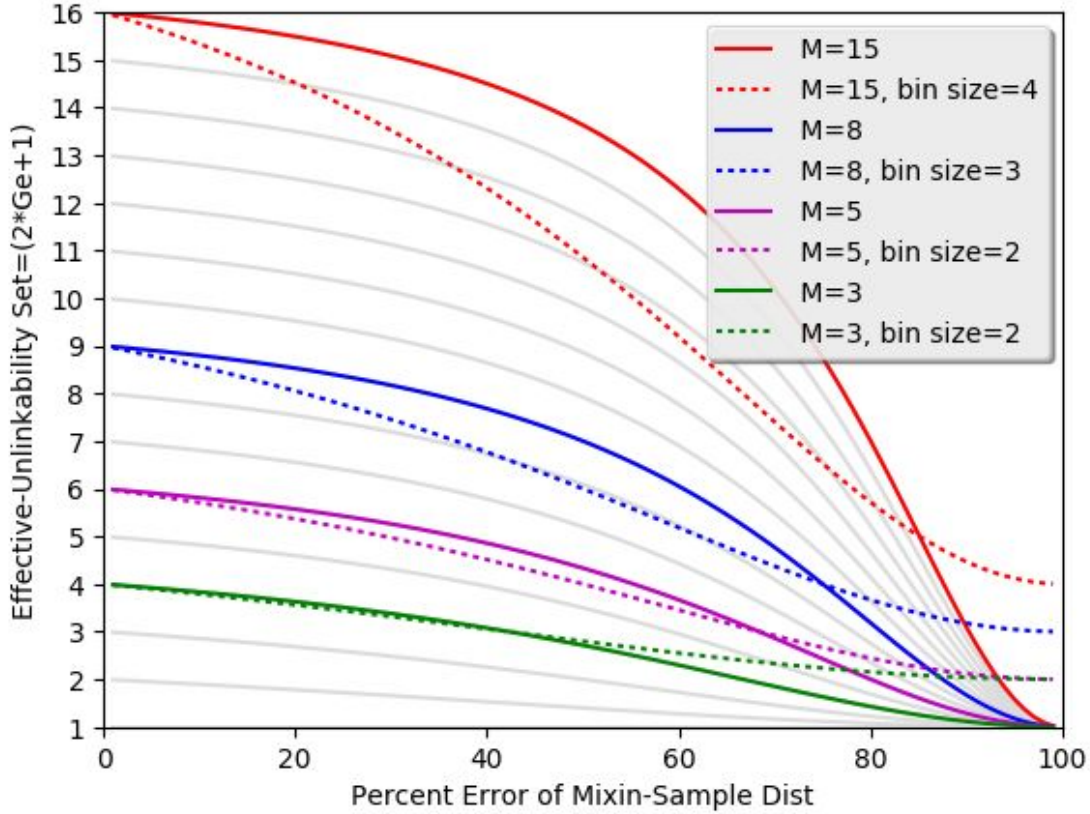
Monero: Singular Mixin Bins (continued)



Monero: Multiple Mixin Bins



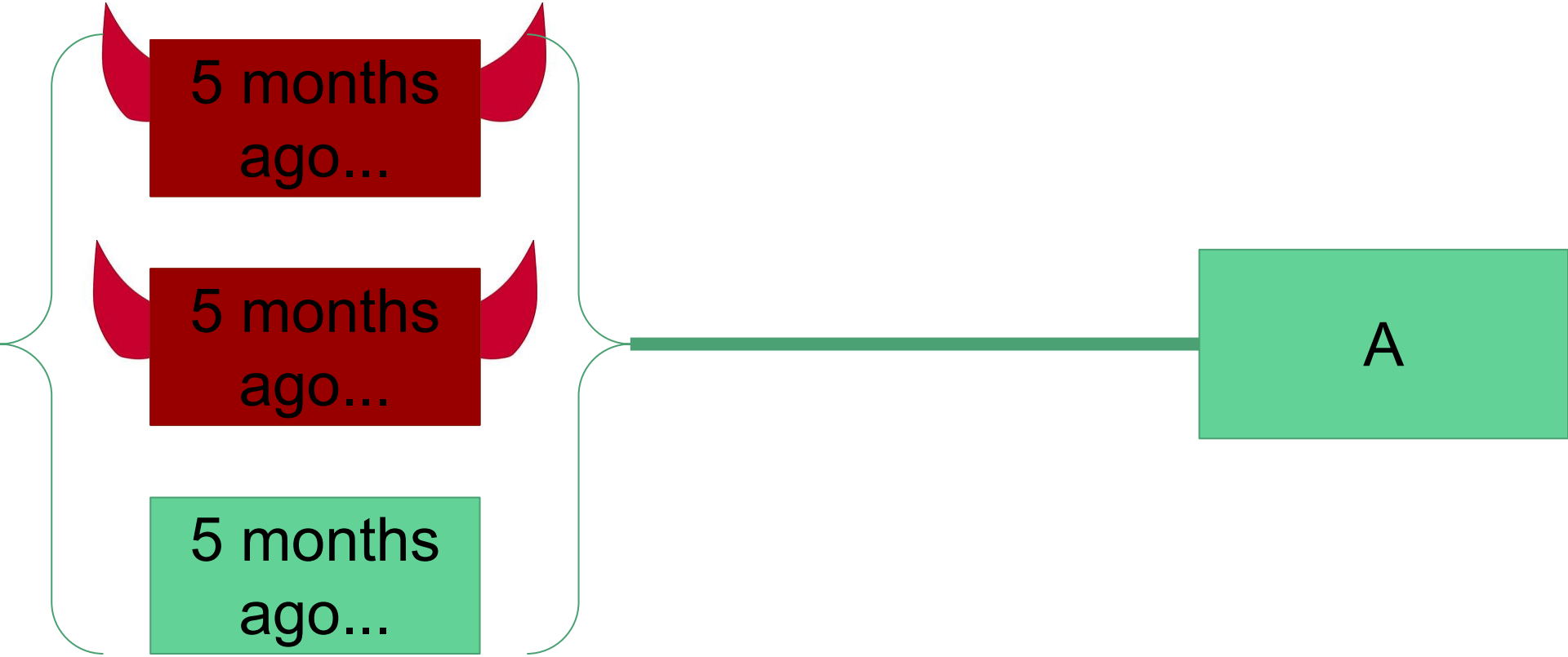
Measuring Anonymity in Bins



Mixin Bins: Advantages and Disadvantages

- Advantages:
  - Defeats temporal analysis
  - Creates a symmetrical system of mixins that has the potential to defeat other attacks as well
  - The stuffing attack, which is discussed afterwards, requires an active attack
- Disadvantages:
  - Is susceptible to the stuffing attack
  - An attacker gains temporal information that might be used in different attacks

Monero: Stuffing Attack

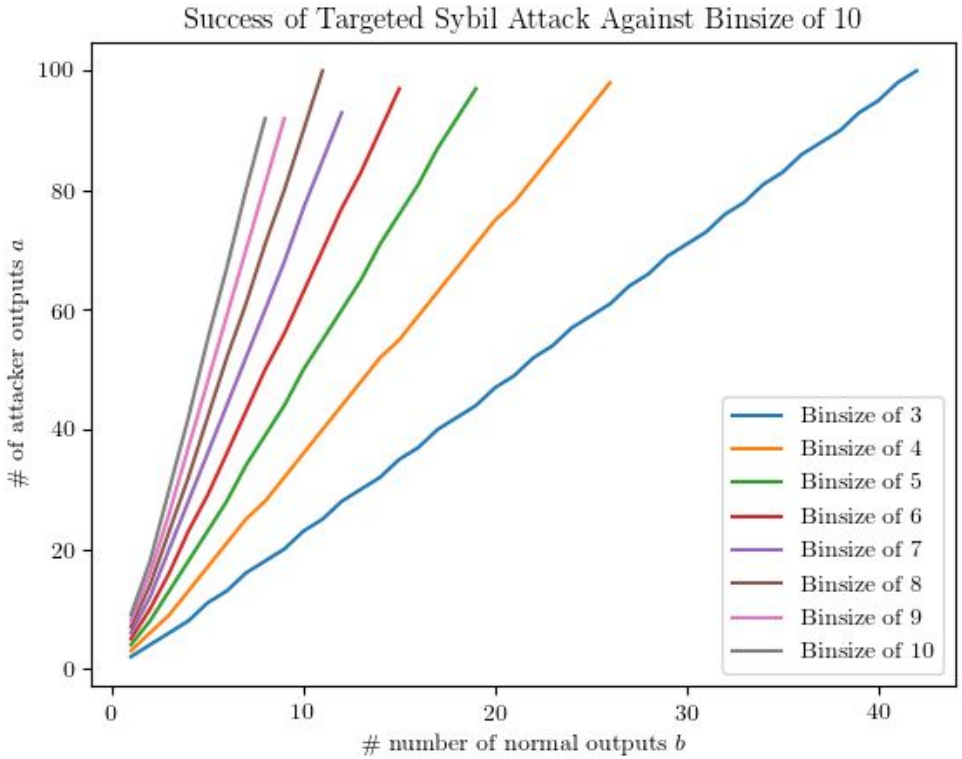


Analysis of the Stuffing Attack

- There are two cases in a stuffing attack
  - Either the attacker wishes to de-anonymize a single node, or the attack wishes to de-anonymize as many nodes as he can, or
  - The attacker may wish to simply deanonymize as many nodes as possible
- We can use a simple random choice model to calculate the probability of success with “a” attacker nodes and “b” normal nodes
  - This may not be an accurate model as attackers may be able to manipulate certain parts of Monero
- We called it a success when a mixin bin is completely compromised

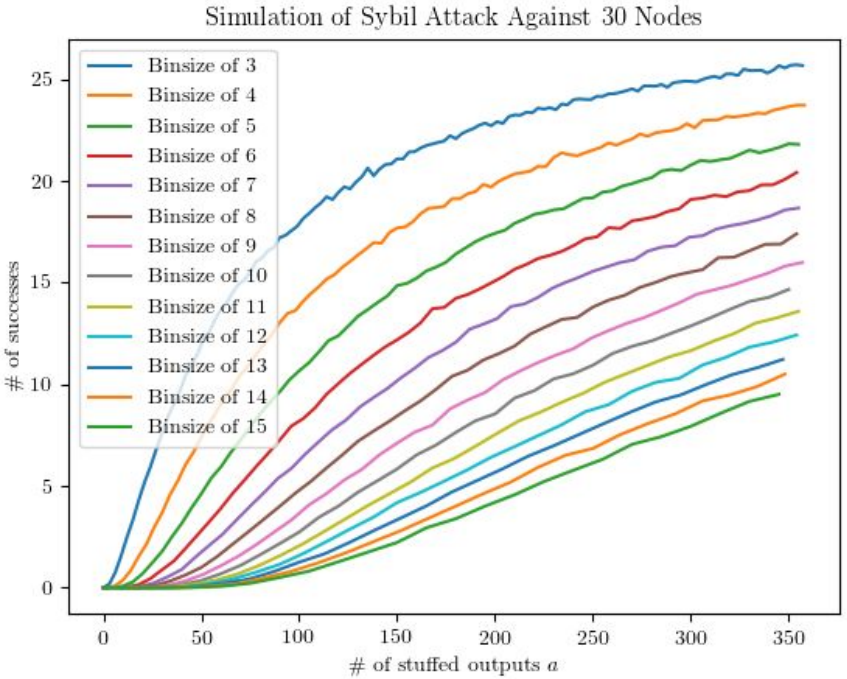
Stuffing Attack - Single Target

$$Pr_{success}(a,b) = \frac{\binom{a}{M-1}}{\binom{a+b-1}{M-1}}$$



Stuffing Attack - Mass-deanonymization

- We simulate the number of success of the number of stuffed attacker nodes to the right
  - Due to the slow nature of cryptographic computations, it may or may not be possible to stuff as many nodes as shown on the right



In our last slide, we would like to thank our mentors: Kyle Hogan, Ethan Heilman, Jason Hennessey, and Mayank Varia.

This talk builds upon the work of [Andrew Miller, Malte Moser, Kevin Lee, Arvind Narayanan]