

# AnonRep: Towards Tracking-Resistant Anonymous Reputation

Ennan Zhai<sup>1</sup>

David Isaac Wolinsky<sup>2</sup>, Ruichuan Chen<sup>3</sup>,

Ewa Syta<sup>1</sup>, Chao Teng<sup>2</sup>, Bryan Ford<sup>4</sup>

<sup>1</sup> Yale <sup>2</sup> Facebook <sup>3</sup> Bell Labs <sup>4</sup> EPFL

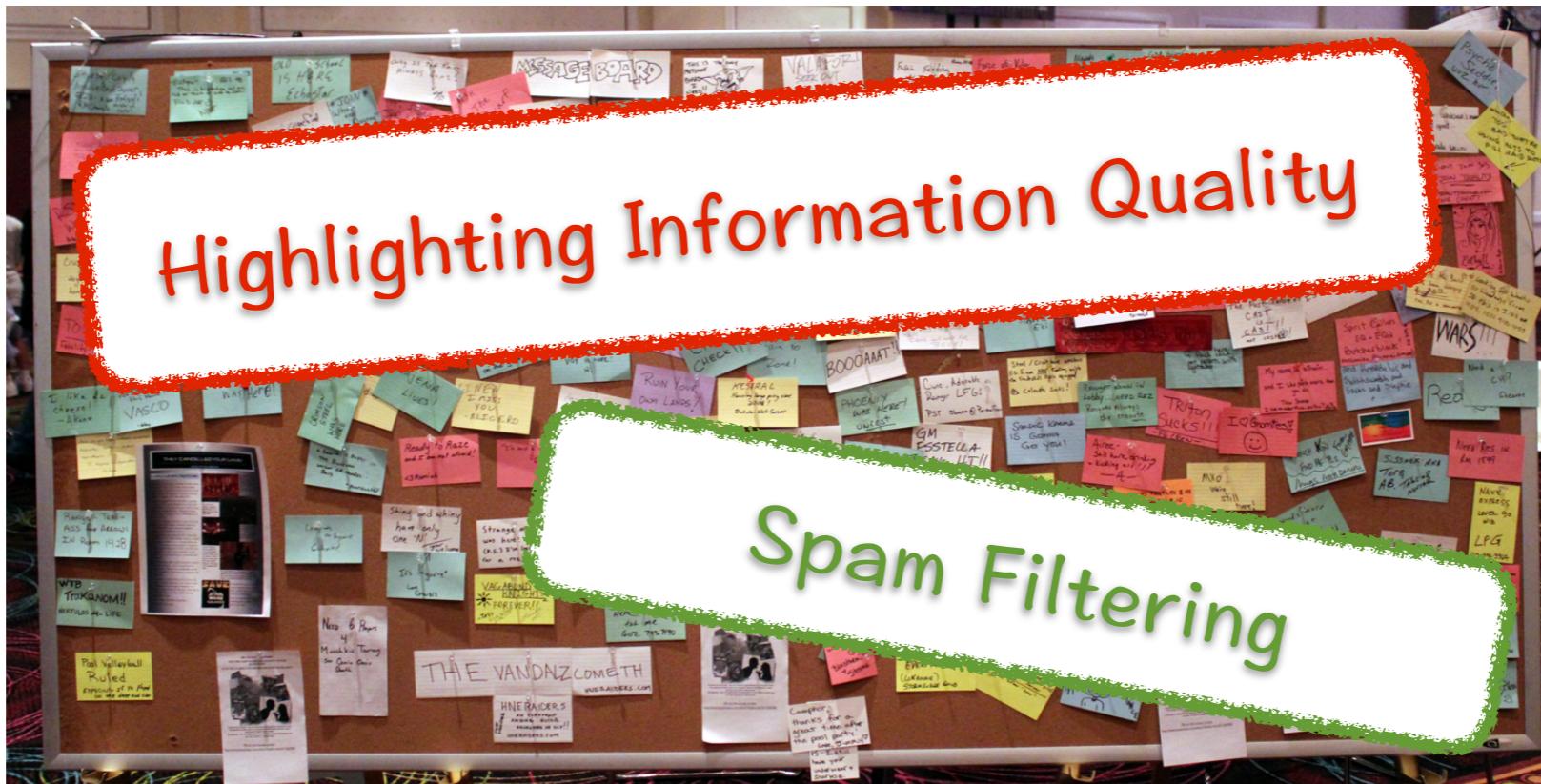
# Background

- There is too much information on today's Internet



# Background

- There is too much information on today's Internet
- Reputation systems are employed:
  - Highlighting information quality
  - Filtering spam



# Stack Overflow

stack overflow

Questions Jobs Tags Users Badges Ask Question

Profile Activity Meta User Network Profile Jon Skeet

REPUTATION  
**849,856**  
top 0.01% overall

850k  
632k  
414k  
2013 2014 2015 2016

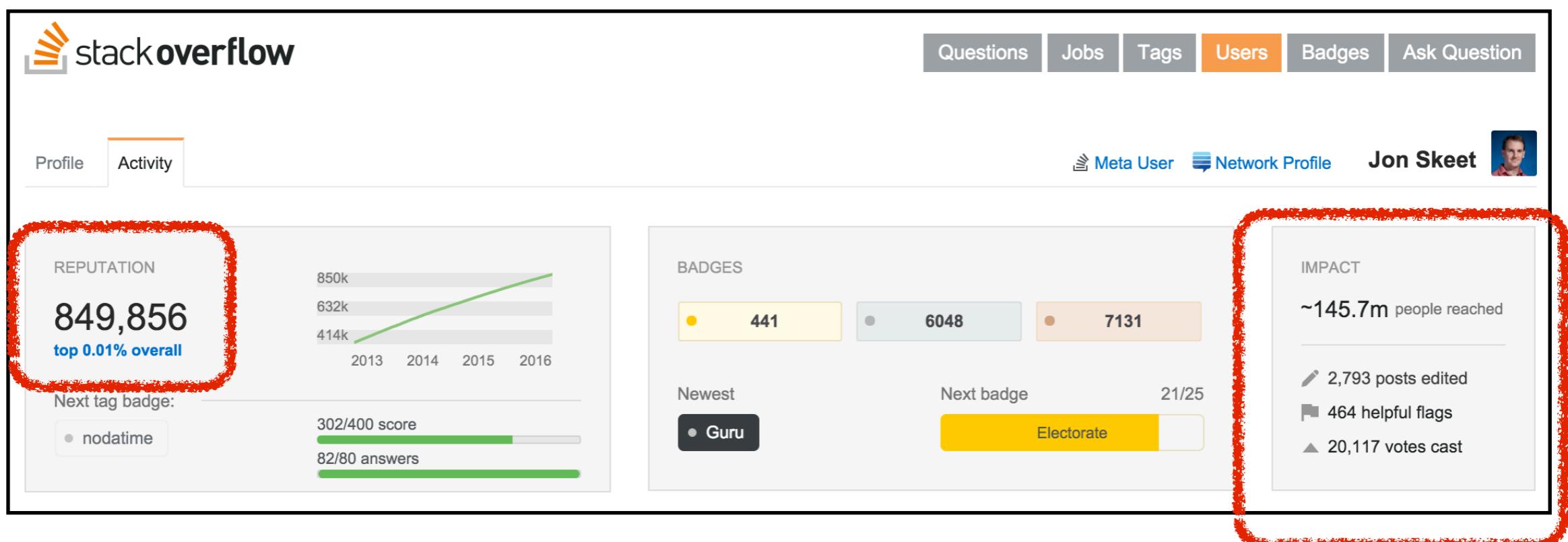
Next tag badge:  
nodatetime

302/400 score  
82/80 answers

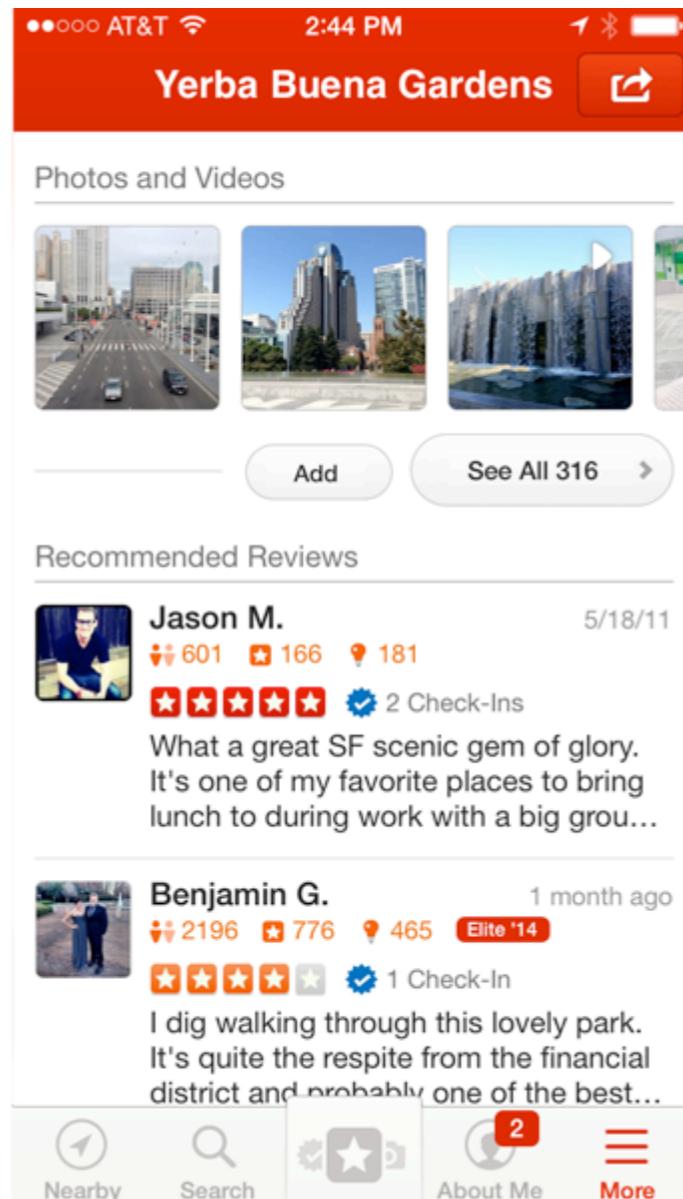
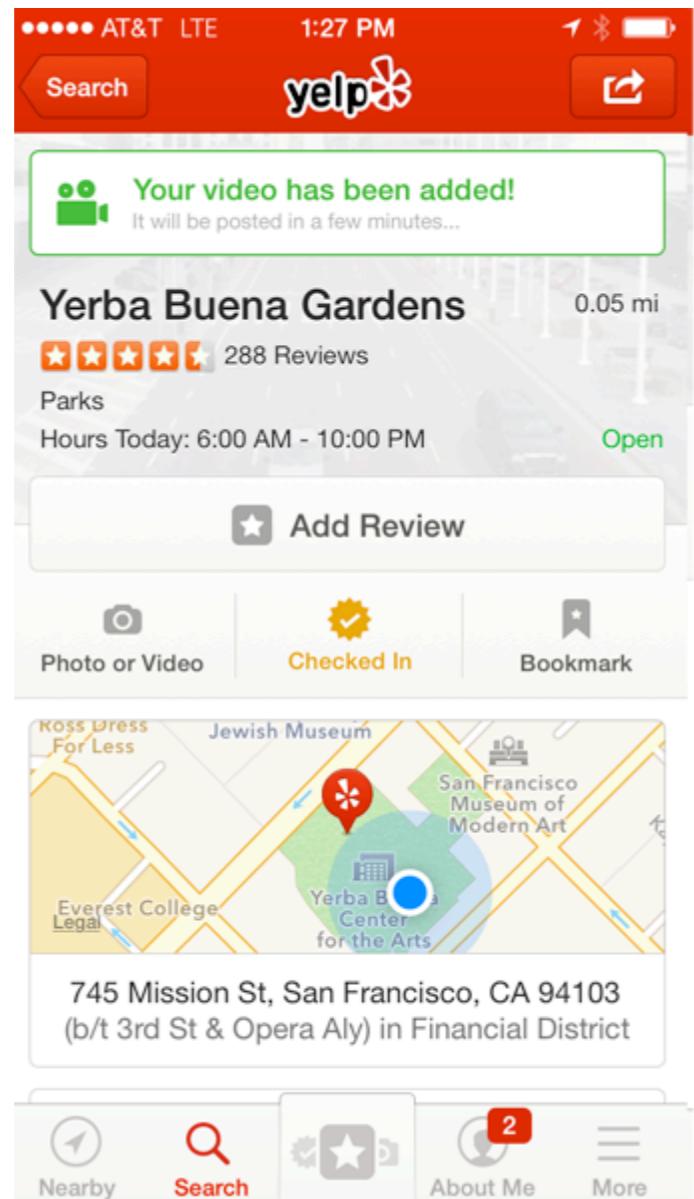
BADGES  
441 6048 7131

Newest Guru Next badge Electorate 21/25

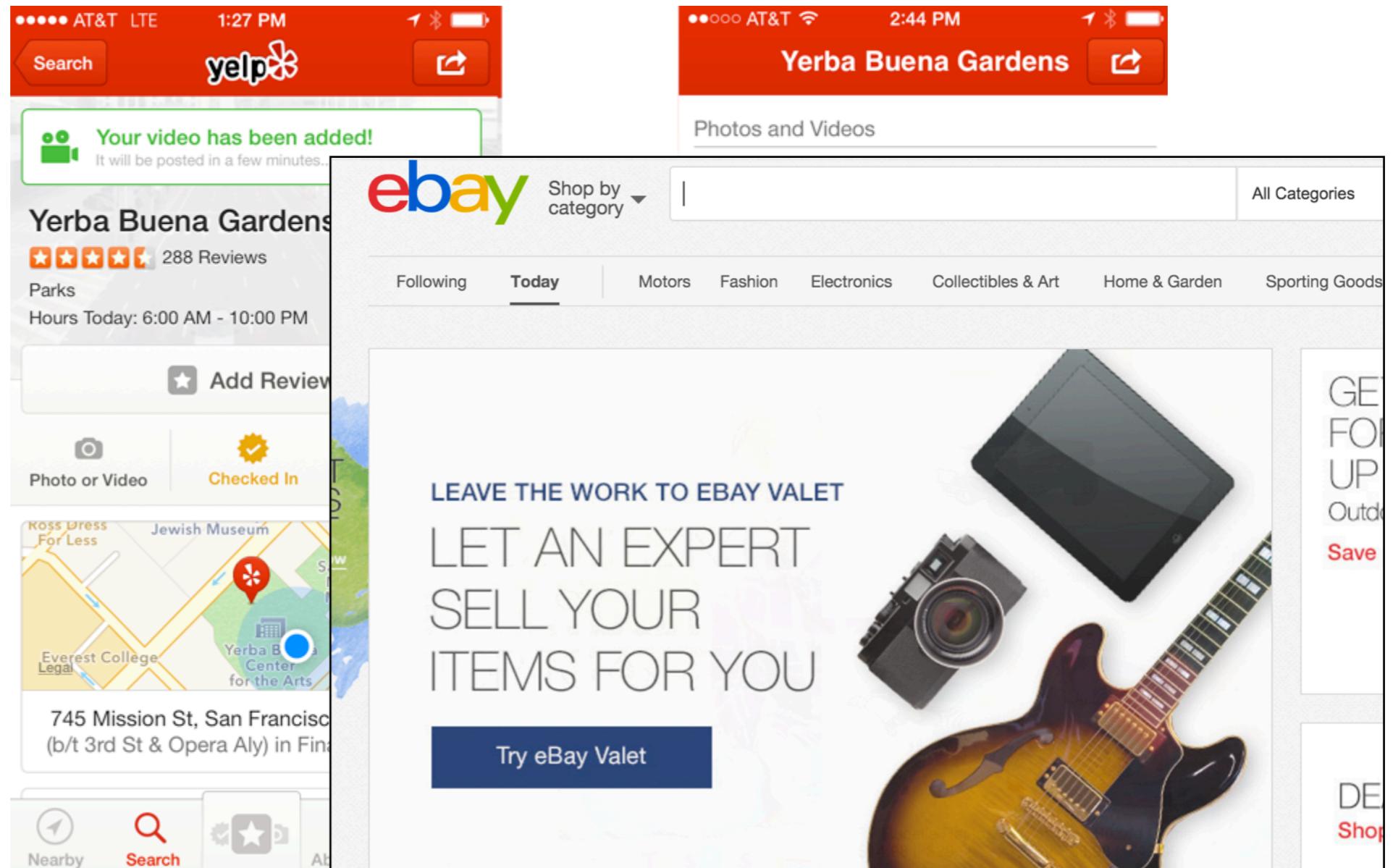
IMPACT  
~145.7m people reached  
2,793 posts edited  
464 helpful flags  
20,117 votes cast



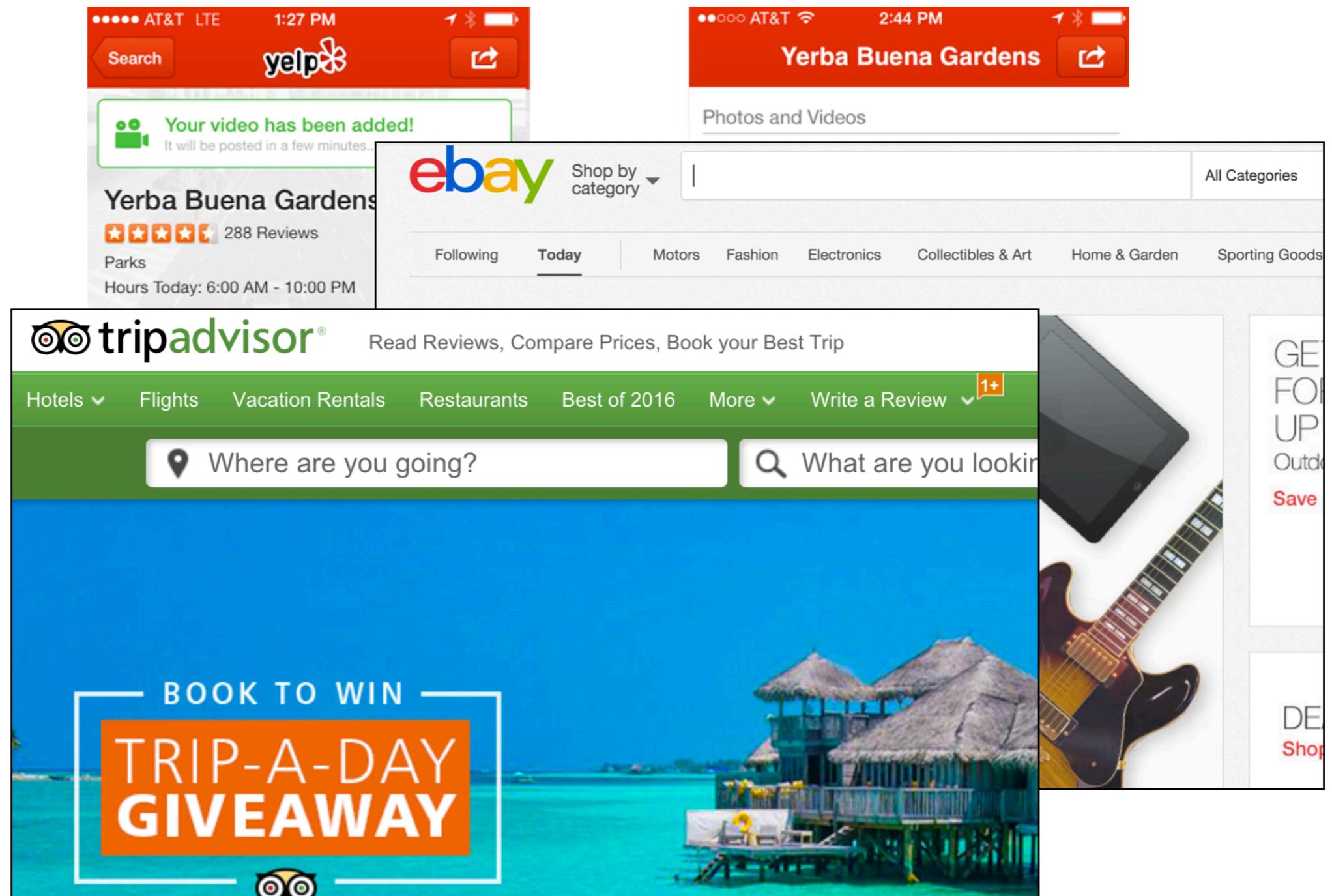
# Reputation System



# Reputation System



# Reputation System



# Reputation System

Messages	Author (Score)	Votes
...	...	
...	...	
...	...	
...	...	

# Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (0)	0
...	...	
...	...	
...	...	

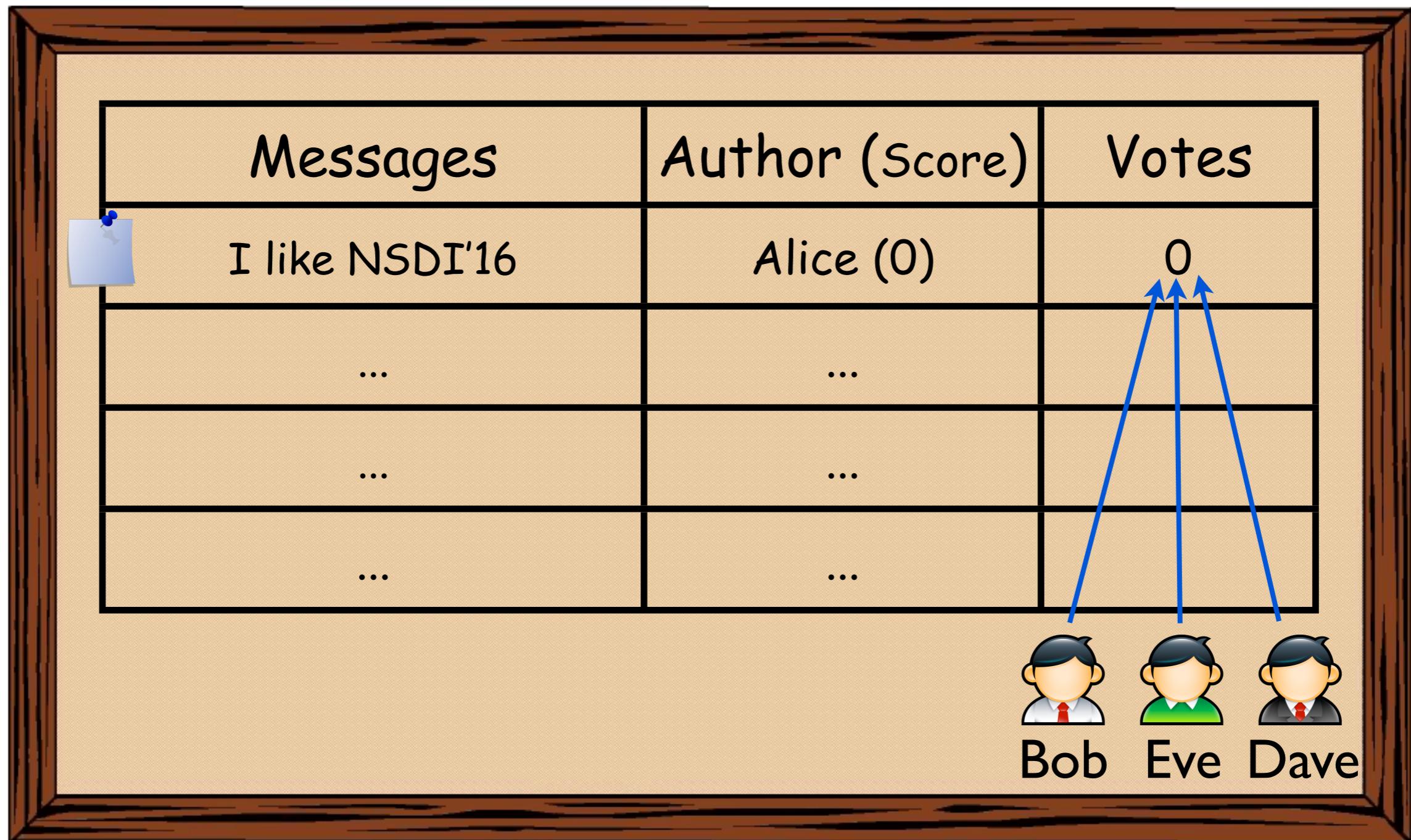
# Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (0)	0
...	...	
...	...	
...	...	

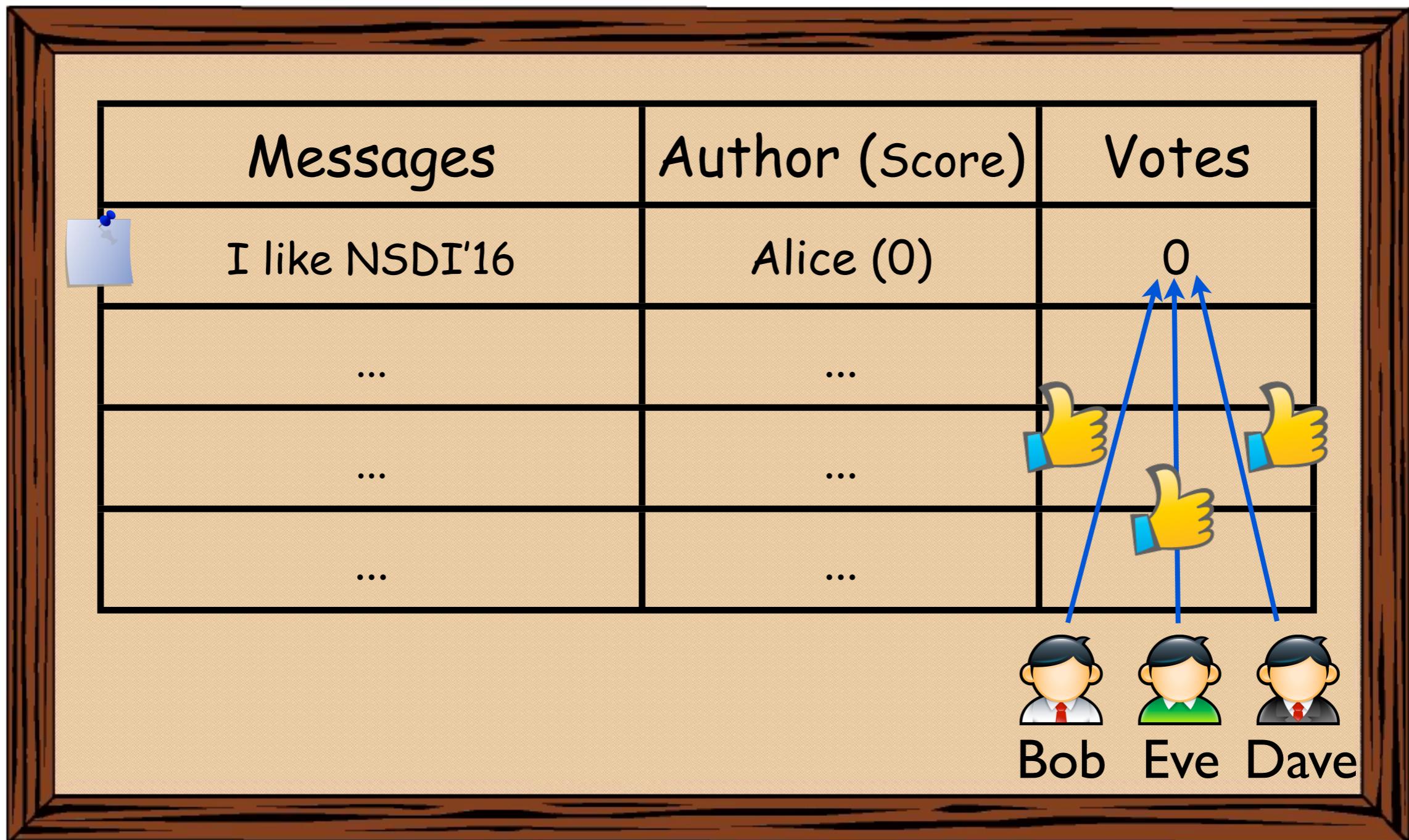
# Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (0)	0
...	...	...
...	...	...
...	...	...

# Reputation System



# Reputation System



# Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (0)	Like: 3
...	...	
...	...	
...	...	



Bob Eve Dave

# Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (3)	Like: 3
...	...	...
...	...	...
...	...	...
$\sum V_i = 1 + 1 + 1 = 3$		 Bob Eve Dave

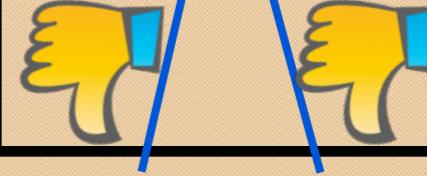
# Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (3)	Like: 3
Don't play with AlphaGo	Alice (3)	0
...	...	
...	...	

# Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (3)	Like: 3
Don't play with AlphaGo	Alice (3)	0
Yale colleges are bad	Bob (1)	0
...	...	

# Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (3)	Like: 3
Don't play with AlphaGo	Alice (3)	0
Yale colleges are bad	Bob (1)	0
...	...	

   
Alice Dave

# Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (3)	Like: 3
Don't play with AlphaGo	Alice (3)	0
Yale colleges are bad	Bob (1)	Dislike: 2
...	...	

   
Alice Dave

# Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (3)	Like: 3
Don't play with AlphaGo	Alice (3)	0
Yale colleges are bad	Bob (-1)	Dislike: 2
...	...	

$\sum V_i = 1 - 1 - 1 = -1$

   
Alice Dave

# People Care About Privacy

- People want to participate in these reputation systems **anonymously** :
  - Sensitive topics
  - Business competitions
  - Other personal concerns

# People Care About Privacy

- People want to participate in these reputation systems

The image displays two side-by-side screenshots. On the left is a TripAdvisor page for the Park Hyatt Sydney. The page shows a banner for 'Traveller Reviews' with a 4.5-star rating. It includes a photo of the hotel's exterior at night, a 'Show Prices' button, and sections for 'Professional photos' and '315 traveller photos'. Below this is a chart of 'Traveller rating' and a section for 'See reviews for' various traveler types. On the right is a Twitter profile for 'Peter Hook @peterchook'. The bio describes him as 'Hugh Grant without the looks or money! Director of propaganda for Accor hotels and resorts in the Asia Pacific' and provides a link to 'accorhotels.com'. The profile shows 5 tweets, 10 following, and 136 followers. Below the bio are three recent tweets from Peter Hook.

**TripAdvisor reviewer**

Park Hyatt Sydney: Traveller Reviews

Ranked #3 of 189 hotels in Sydney

558 Reviews

See lowest price for your stay\*

Show Prices

Professional photos

315 traveller photos

Traveller Reviews Room Prices

558 reviews from our community Write a Review

Traveller rating

Rating	Count
Excellent	417
Very good	88
Average	26
Poor	16
Terrible	11

See what rooms travellers prefer - 106 traveller tips

**Peter Hook**  
@peterchook  
Hugh Grant without the looks or money! Director of propaganda for Accor hotels and resorts in the Asia Pacific  
Sydney · accorhotels.com

5 TWEETS 10 FOLLOWING 136 FOLLOWERS Follow

**Tweets**

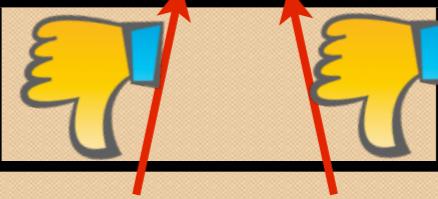
Peter Hook @peterchook What Sydney hotel has the best view from a bath? 2 May  
@SebelPierOne @AccorAustralia pic.twitter.com/C9tDwutOpJ  
View photo

Peter Hook @peterchook @Angela\_Saune Hear you slept in the same bedroom as Robert Redford and Keith Urban at Pullman Brisbane. Hope they didn't keep you awake. 2 May  
View conversation

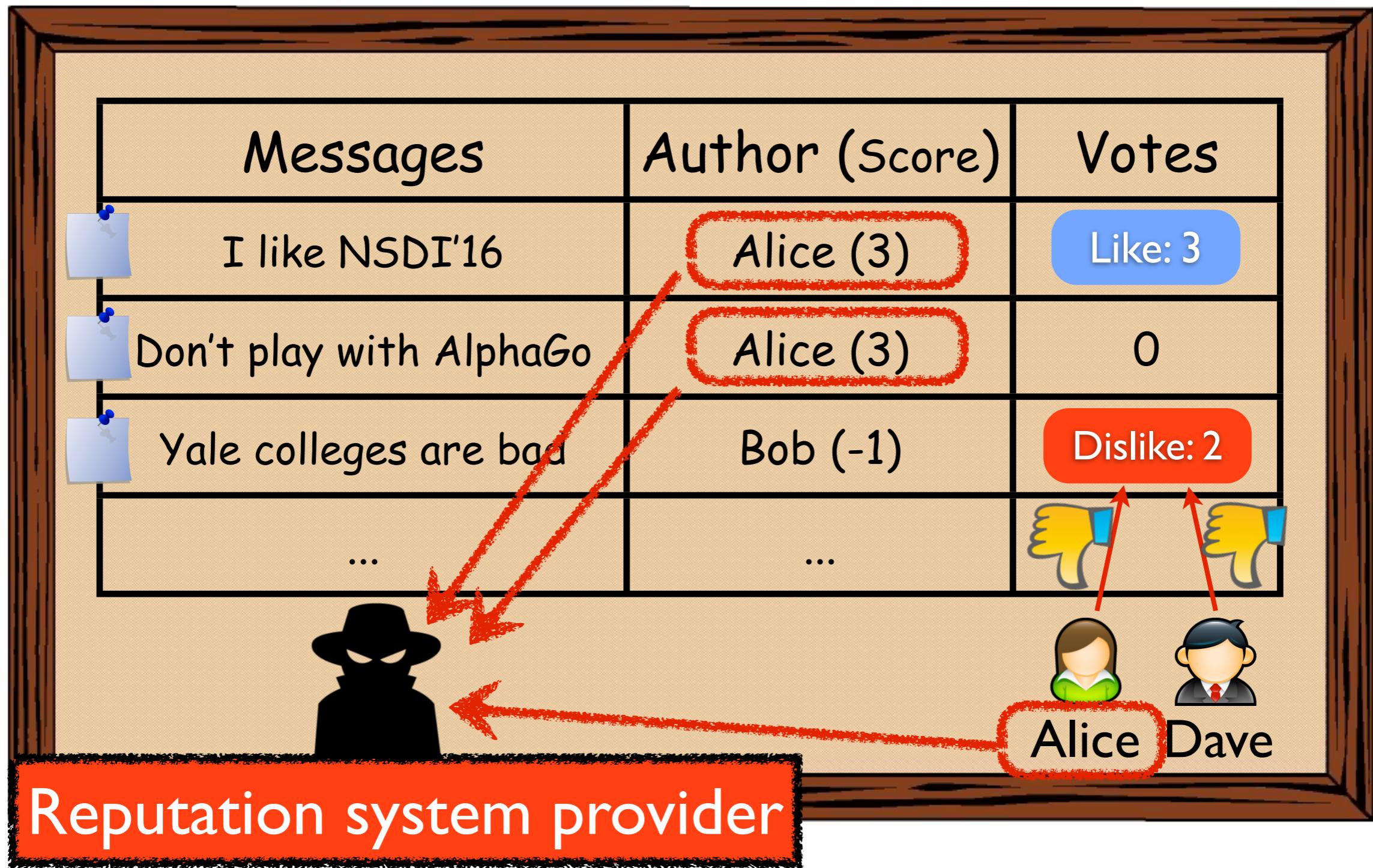
Peter Hook @peterchook There's much more to #Queensland than sun & surf... now 5 Apr 11

# TARGET: Linkability Problem

# TARGET: Linkability Problem

Messages	Author (Score)	Votes
I like NSDI'16	Alice (3)	Like: 3
Don't play with AlphaGo	Alice (3)	0
Yale colleges are bad	Bob (-1)	Dislike: 2
...	...	
	Alice Dave	

# TARGET: Linkability Problem



# TARGET: Linkability Problem

## I Know What You're Buying: Privacy Breaches on eBay

Tehila Minkus<sup>1</sup> and Keith W. Ross<sup>1,2</sup>

<sup>1</sup> Dept. of Computer Science and Engineering, NYU

<sup>2</sup> NYU Shanghai

[tehila@nyu.edu](mailto:tehila@nyu.edu), [keithwross@nyu.edu](mailto:keithwross@nyu.edu)



Alice Dave

# Anonymous Reputation System

**Reputation system provider** and **any user**

should not be able to link any user's activities

# Existing Efforts

- E-Cash based approaches [1]:
  - Only support positive feedback
  - Not support diverse reputation algorithms

[1] John Bethencourt et al. Signatures of reputation. In FC'10.

# Existing Efforts

- E-Cash based approaches [1]:
  - Only support positive feedback
  - Not support diverse reputation algorithms
- Blind signature-based efforts [2]:
  - Also limited to positive feedback
  - Need a centralized banker

[1] John Bethencourt et al. Signatures of reputation. In FC'10.

[2] Elli Androulaki et al. Reputation systems for anonymous networks. In PETS'08.

# Existing Efforts

- E-Cash based approaches [1]:
  - Only support positive feedback
  - Not support diverse reputation algorithms
- Blind signature-based efforts [2]:
  - Also limited to positive feedback
  - Need a centralized banker

The primitives they depend on are computationally expensive!

[1] John Bethencourt et al. Signatures of reputation. In FC'10.

[2] Elli Androulaki et al. Reputation systems for anonymous networks. In PETS'08.

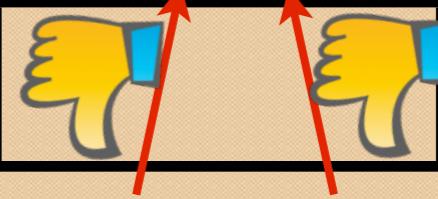
# Our Goals

- Tracking-resistant anonymous reputation:
  - Unlinkability and anonymity of users' activities
  - Diverse reputation utilities (algorithms)

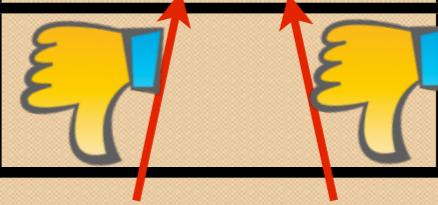
# Our Goals

- Tracking-resistant anonymous reputation:
  - Unlinkability and anonymity of users' activities
  - Diverse reputation utilities (algorithms)
  - No need trust any centralized party
  - Scalable to large-size user set

# Example

Messages	Author (Score)	Votes
I like NSDI'16	Alice (3)	Like: 3
Don't play with AlphaGo	Alice (3)	0
Yale colleges are bad	Bob (-1)	Dislike: 2
...	...	
	Alice Dave	

# Example

Messages	Author (Score)	Votes
I like NSDI'16	xowa (3)	Like: 3
Don't play with AlphaGo	f891 (3)	0
Yale colleges are bad	3fio (-1)	Dislike: 2
...	...	
	 k892 ji12	

# Technical Challenges

# Technical Challenges

- Reputation update relies on activities tracking

It is a paradox in practice!

# Technical Challenges

- Reputation update relies on activities tracking
- Misbehaviors (e.g., duplicate voting) detection

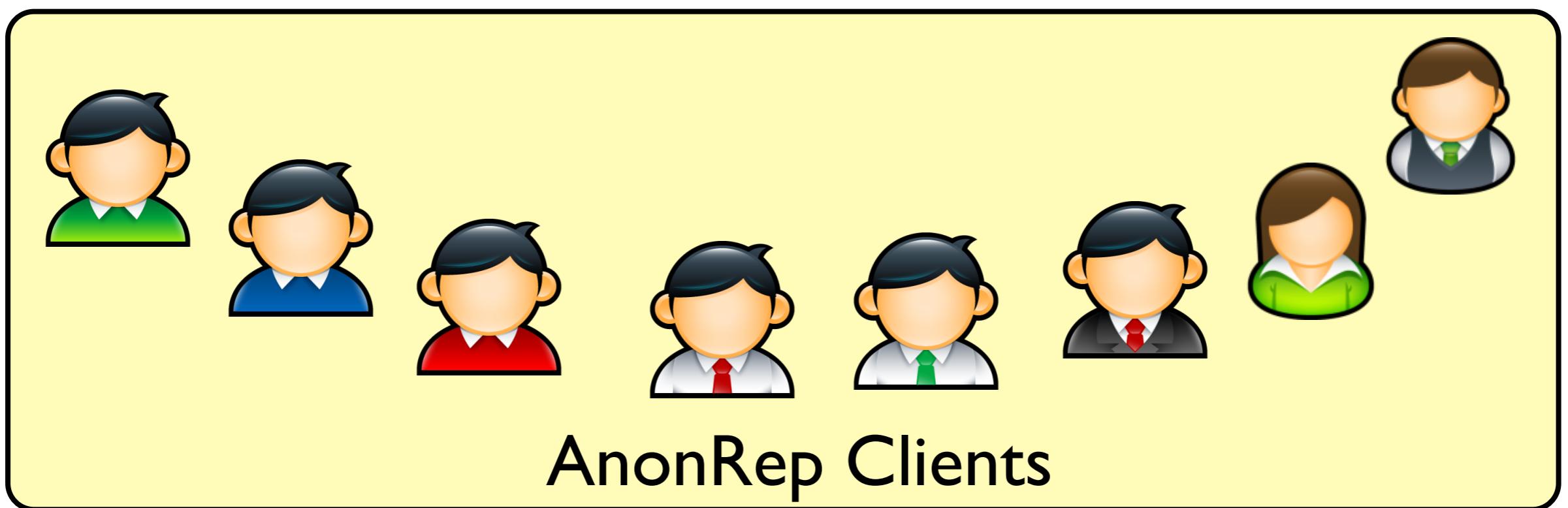
# Road-Map

- Motivations
- AnonRep Design
- Practical Considerations
- Evaluation

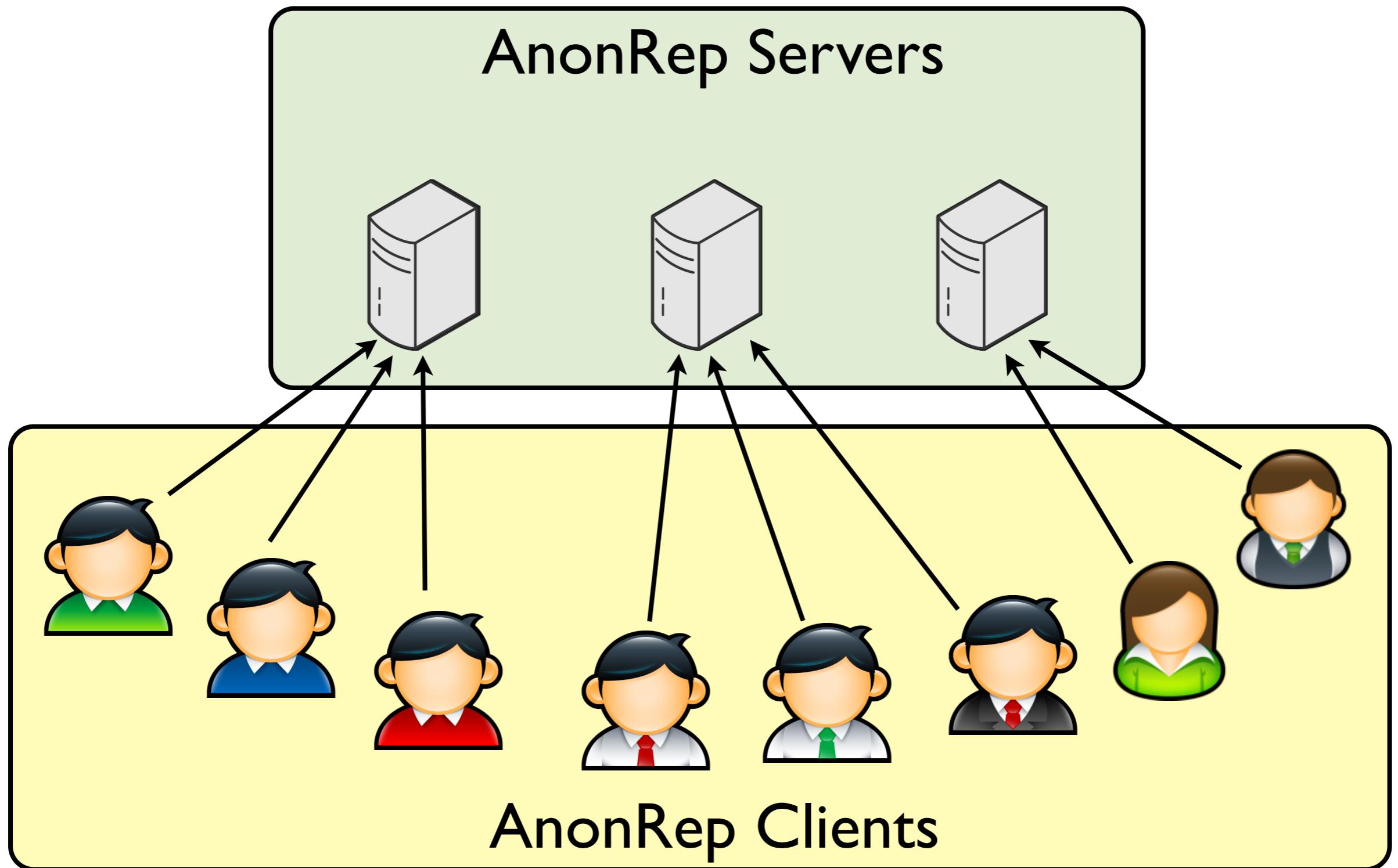


# AnonRep Deployment

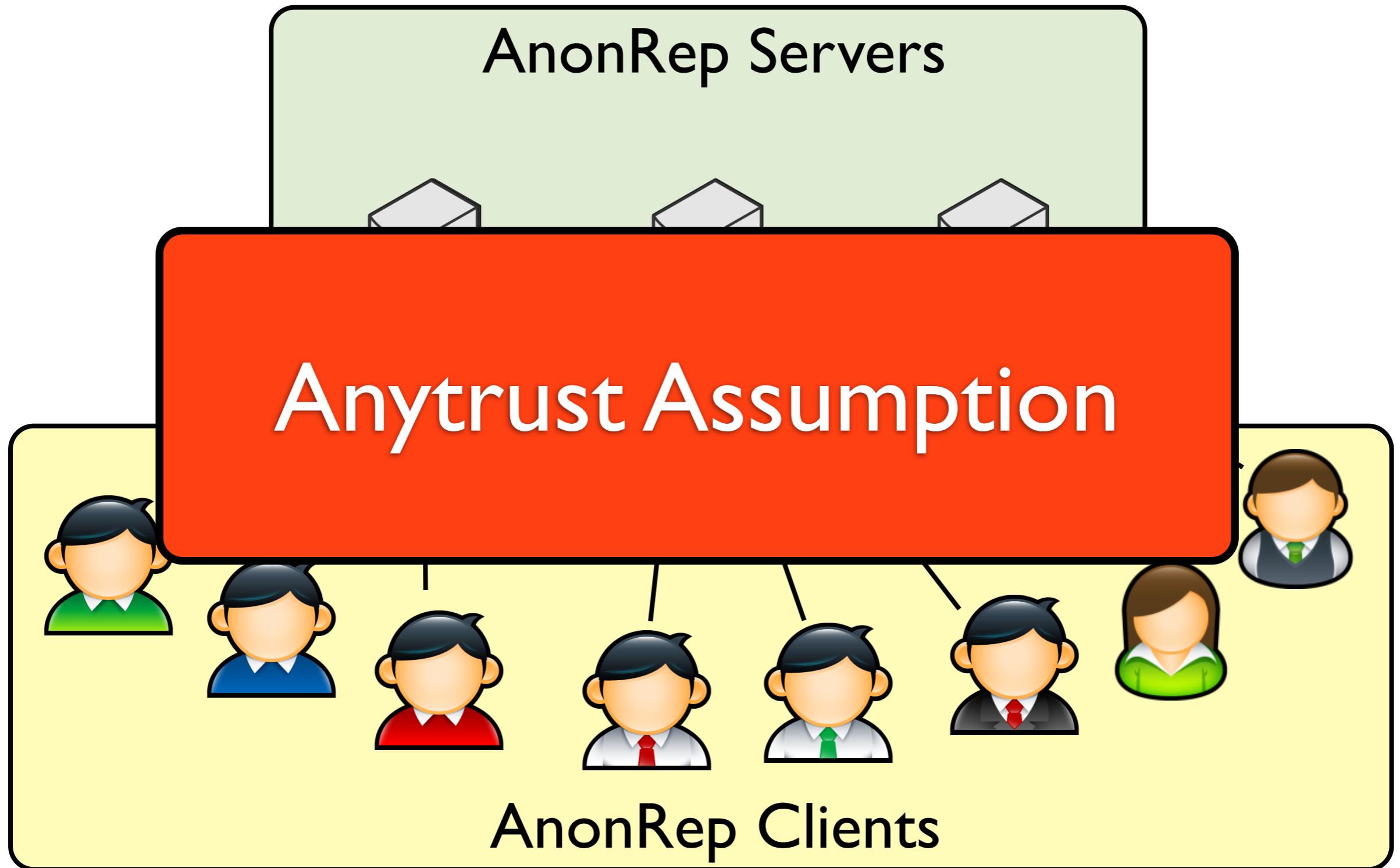
# AnonRep Deployment



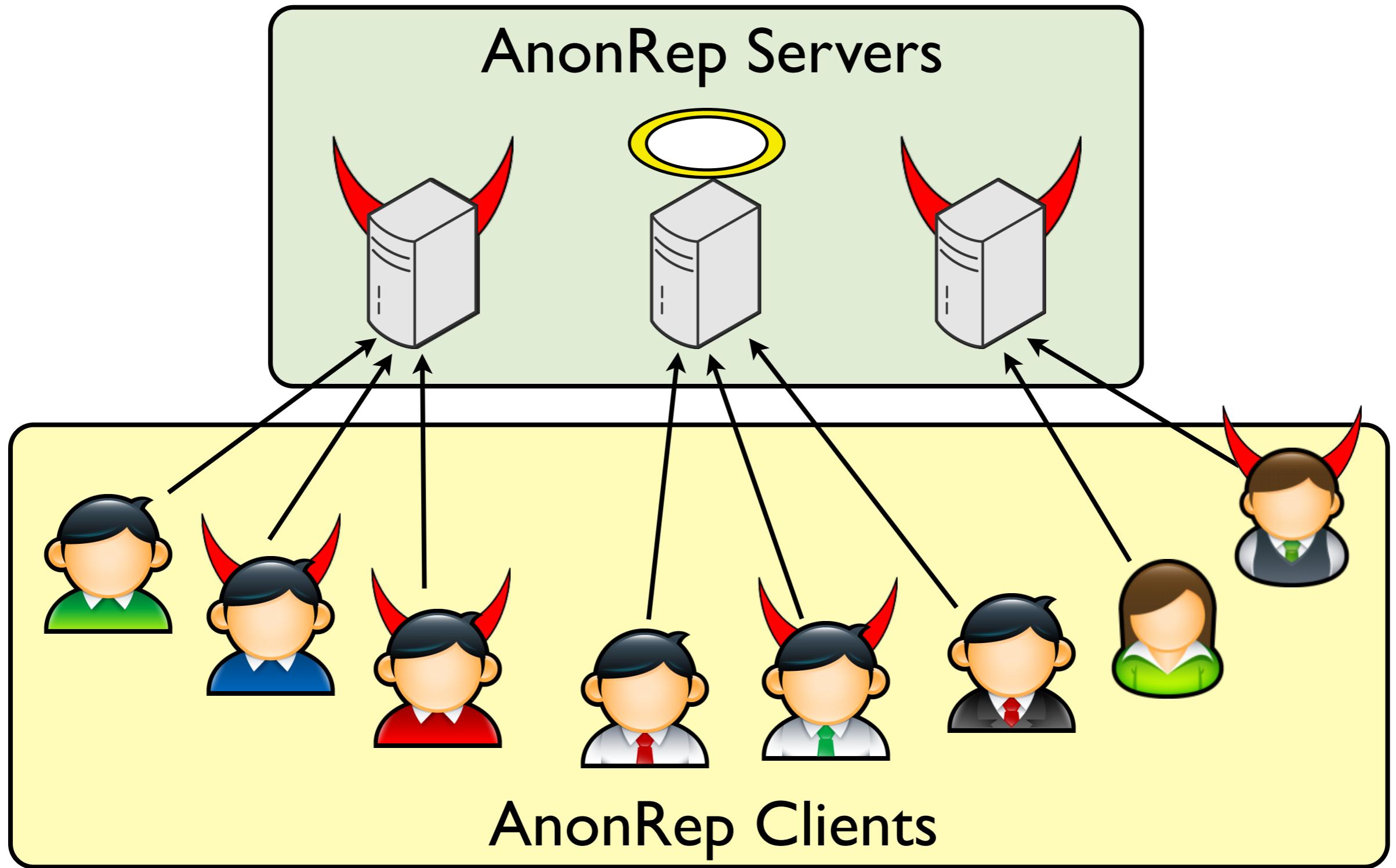
# AnonRep Deployment



# Threat Model

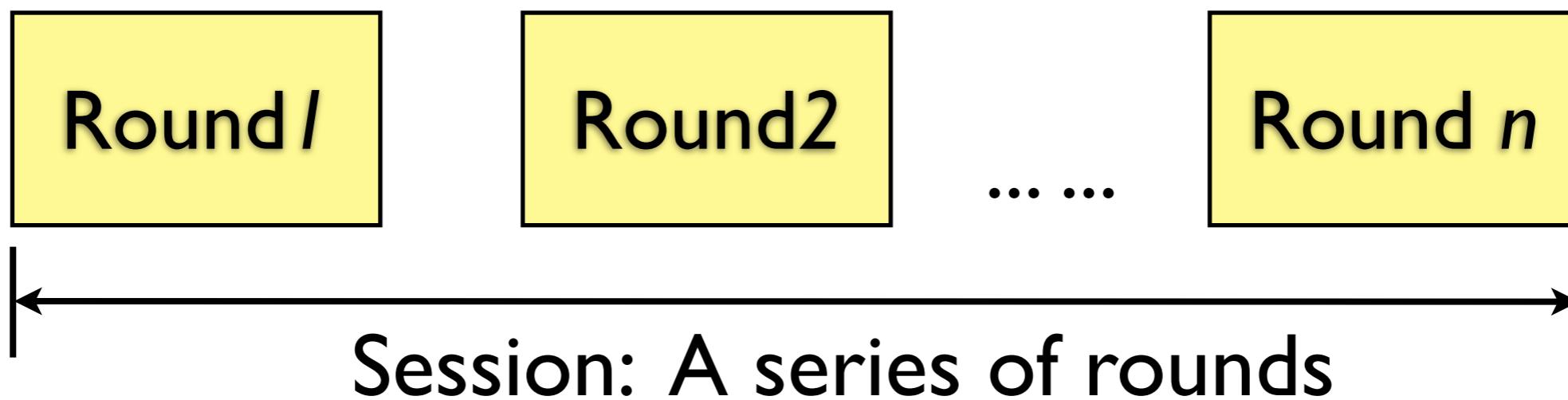


# Threat Model



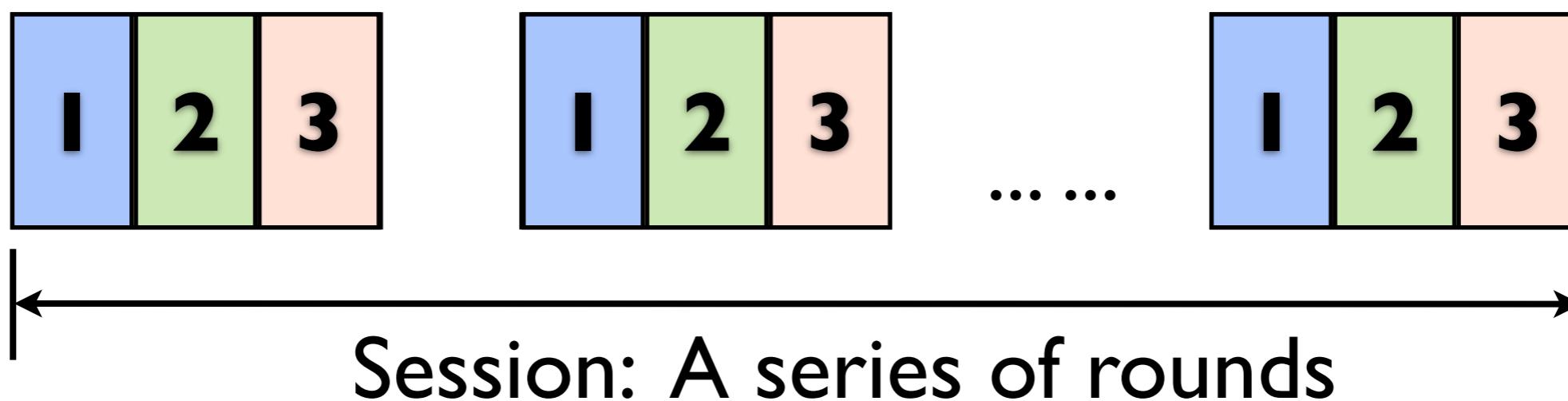
# AnonRep Workflow

- Members (including servers and clients) participate in a continuous series of rounds

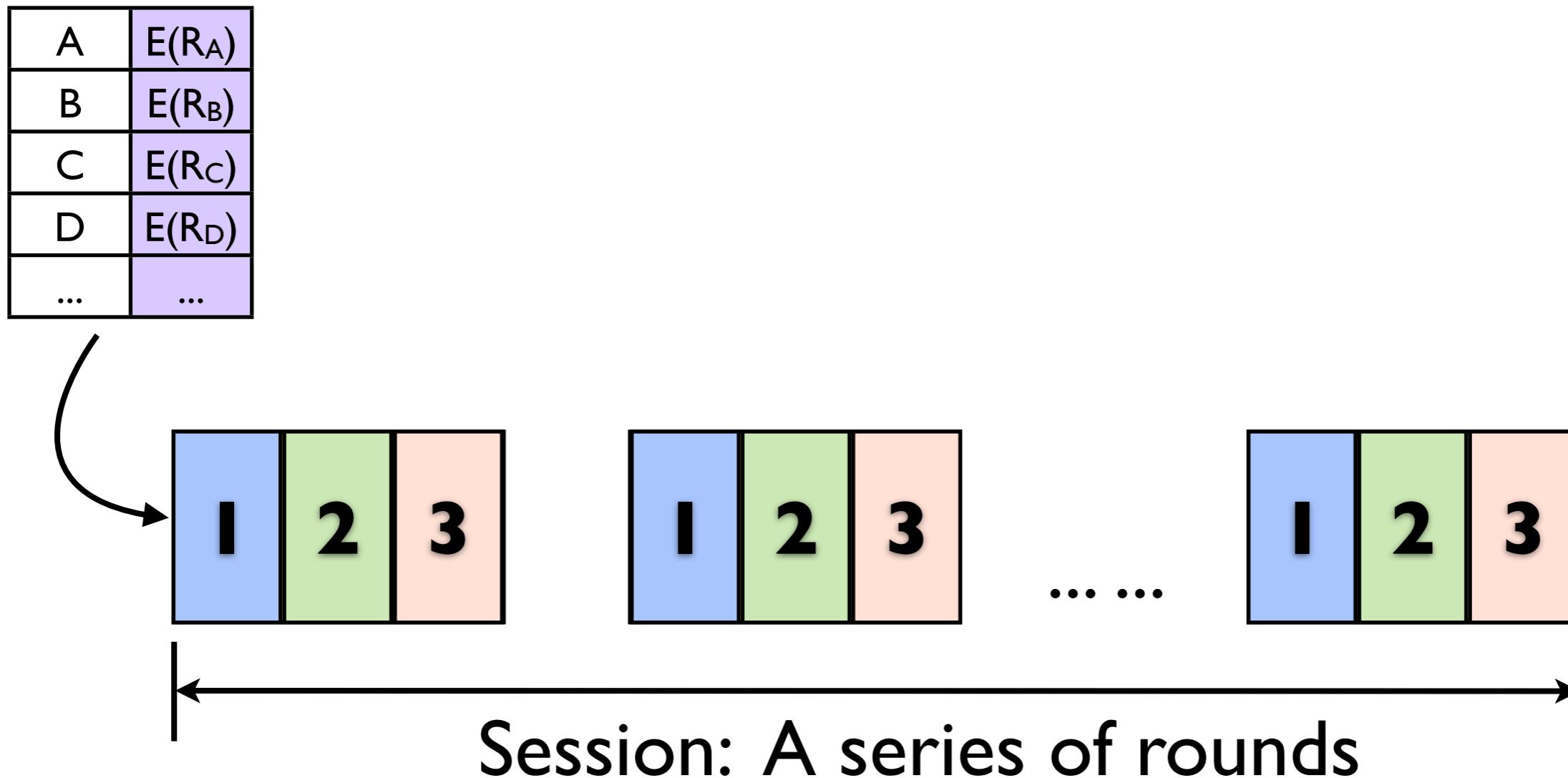


# AnonRep Workflow

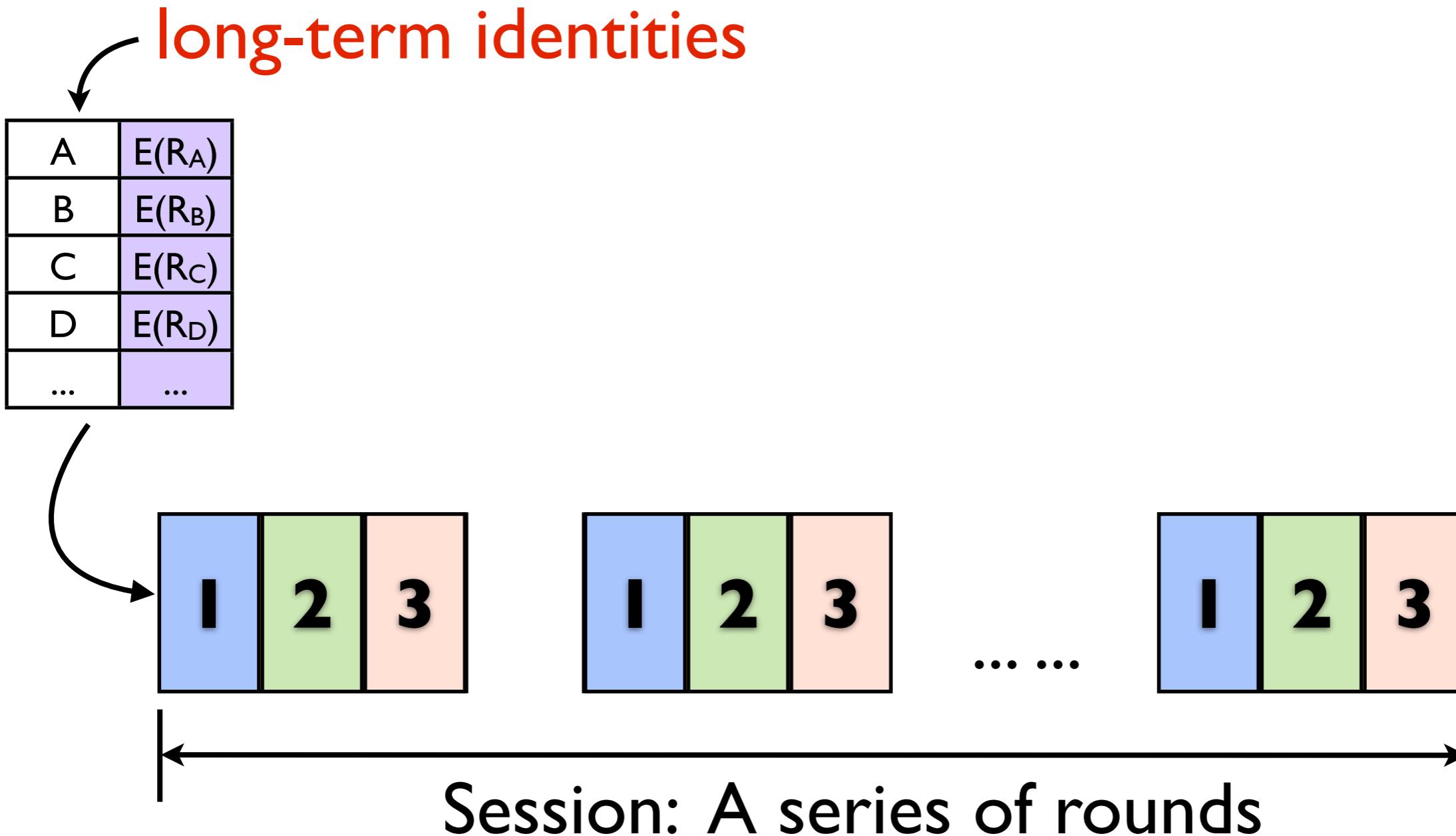
- Each round has three steps
  - Step1: Announcement
  - Step2: Message postings
  - Step3: Feedback collection



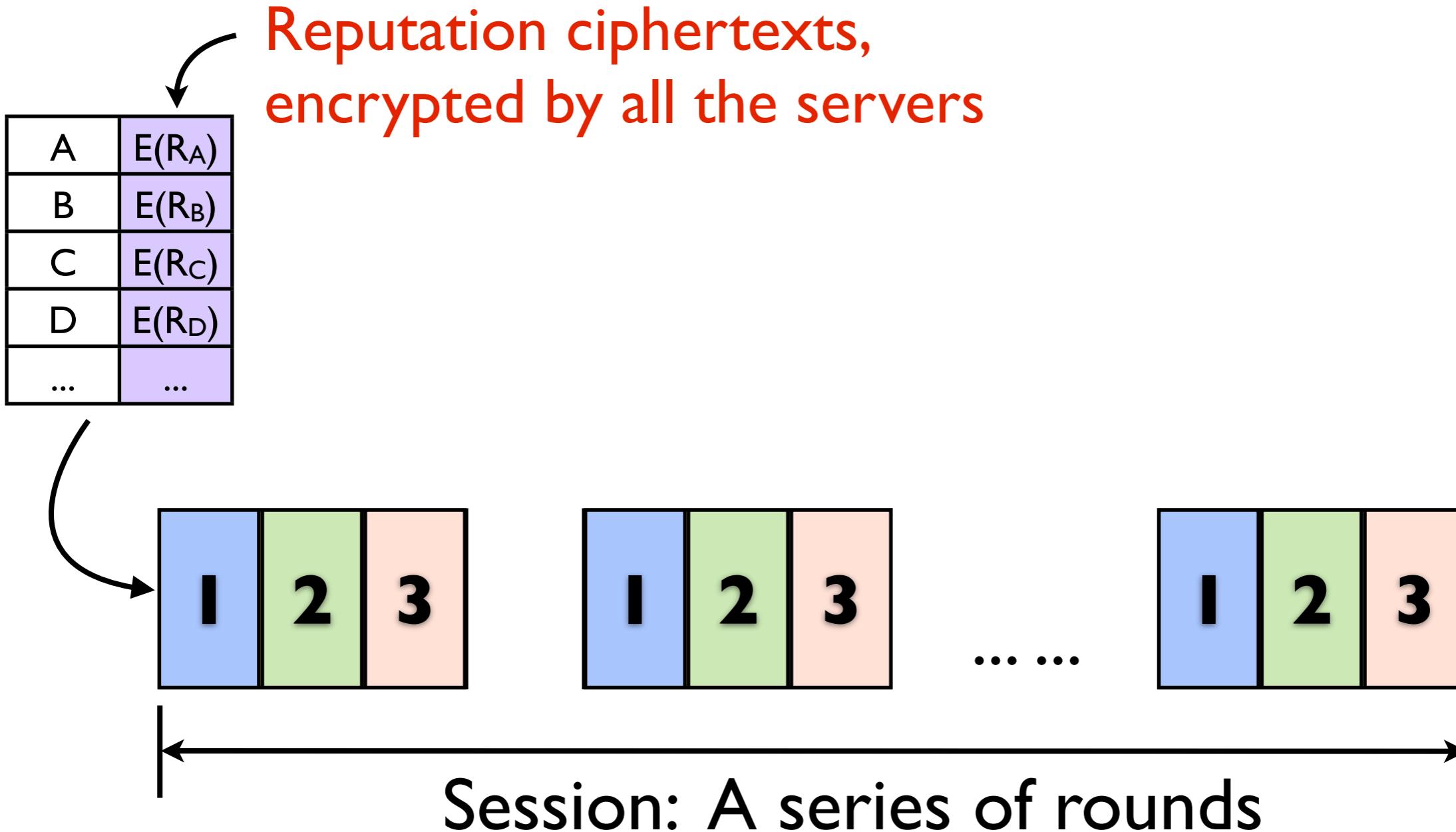
# AnonRep Workflow



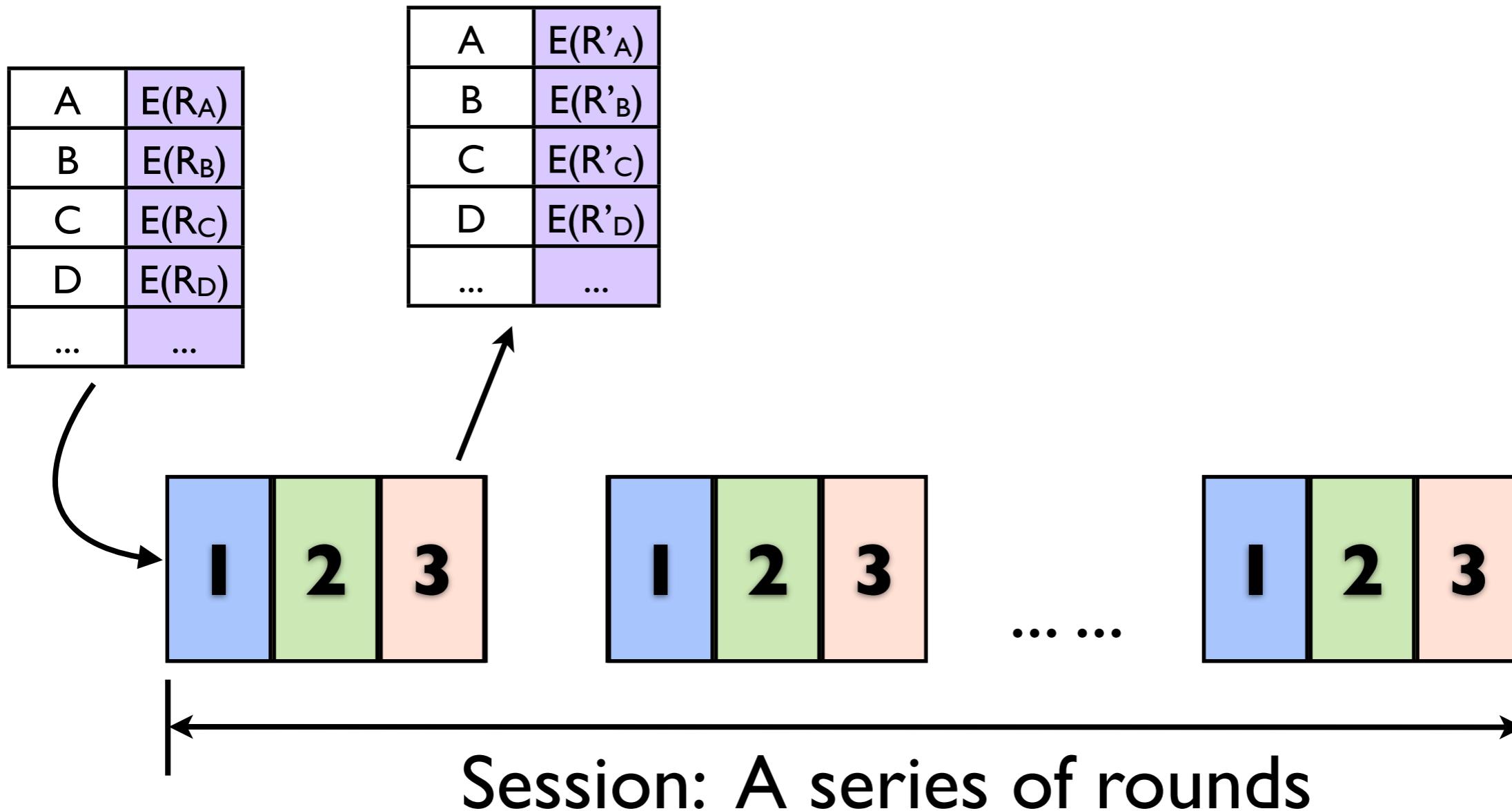
# AnonRep Workflow



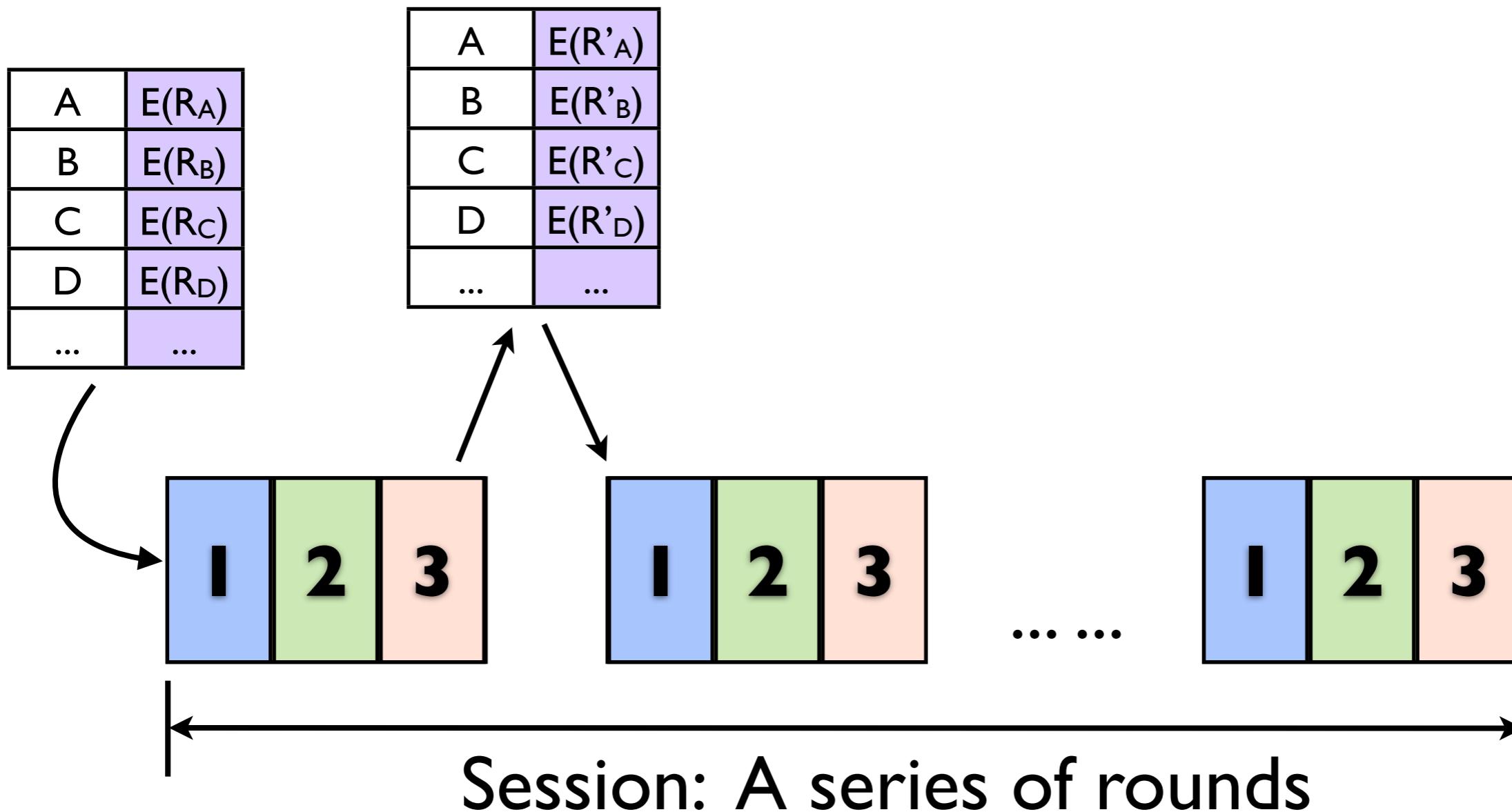
# AnonRep Workflow



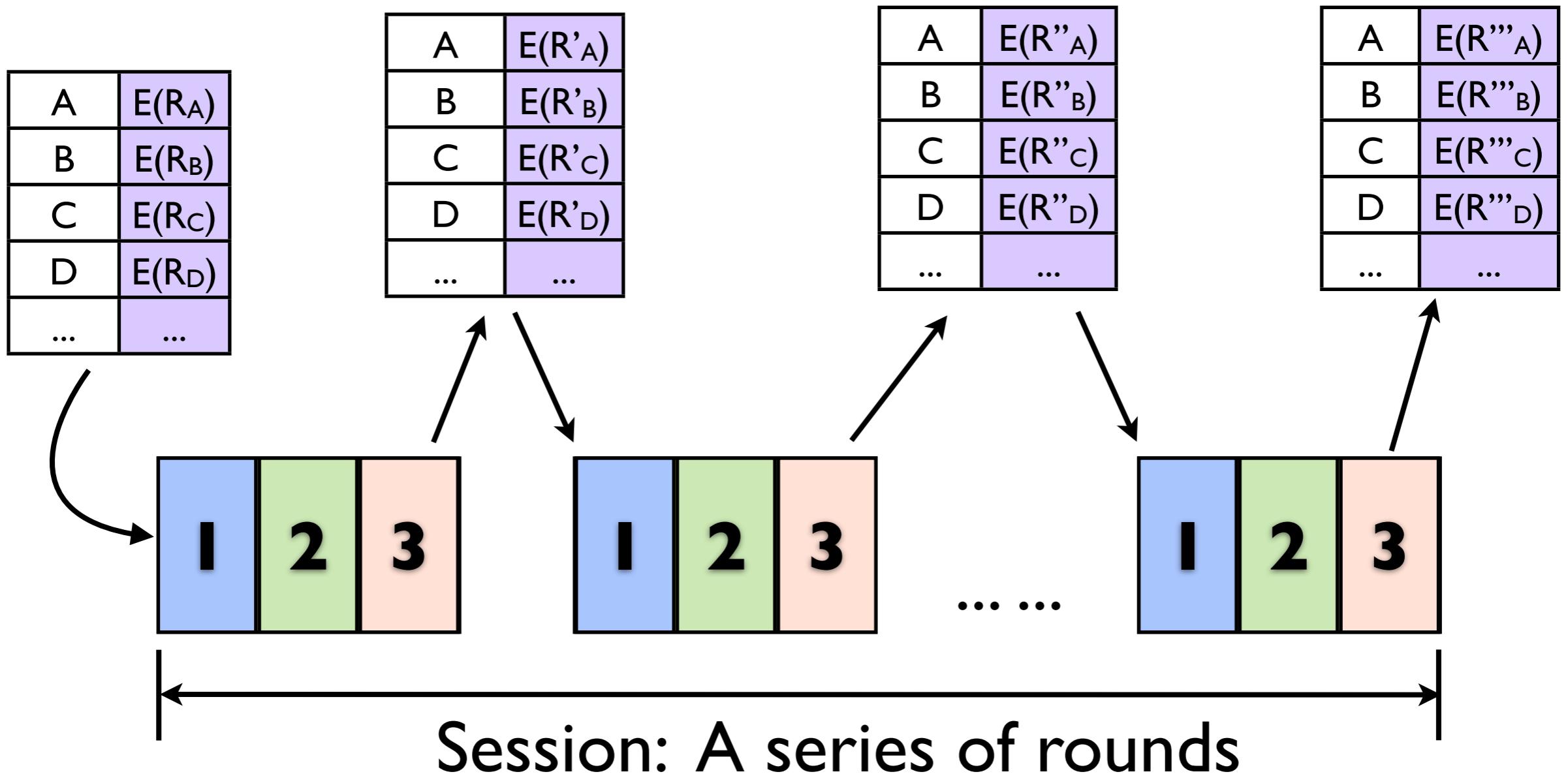
# AnonRep Workflow



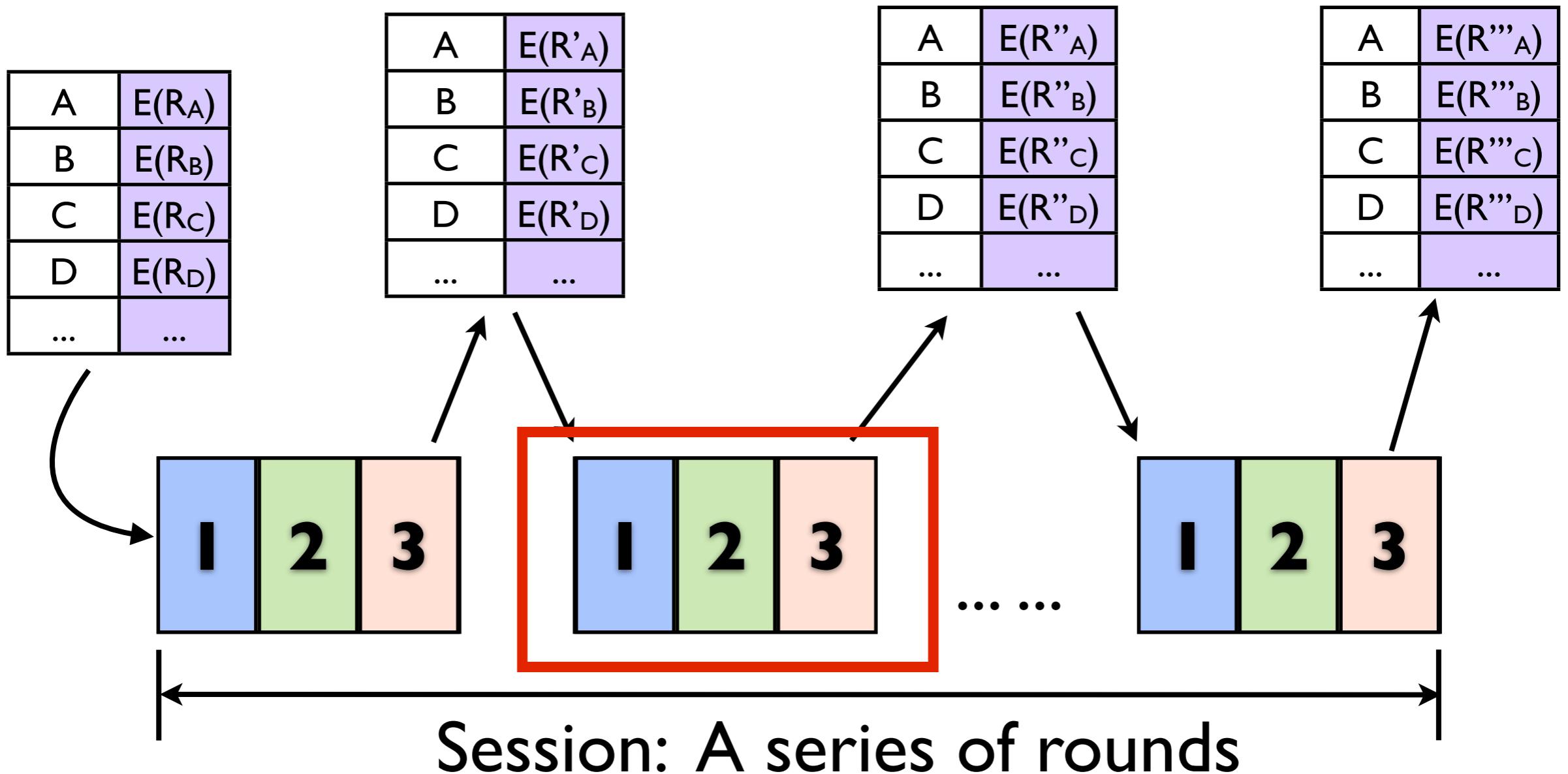
# AnonRep Workflow



# AnonRep Workflow



# AnonRep Workflow



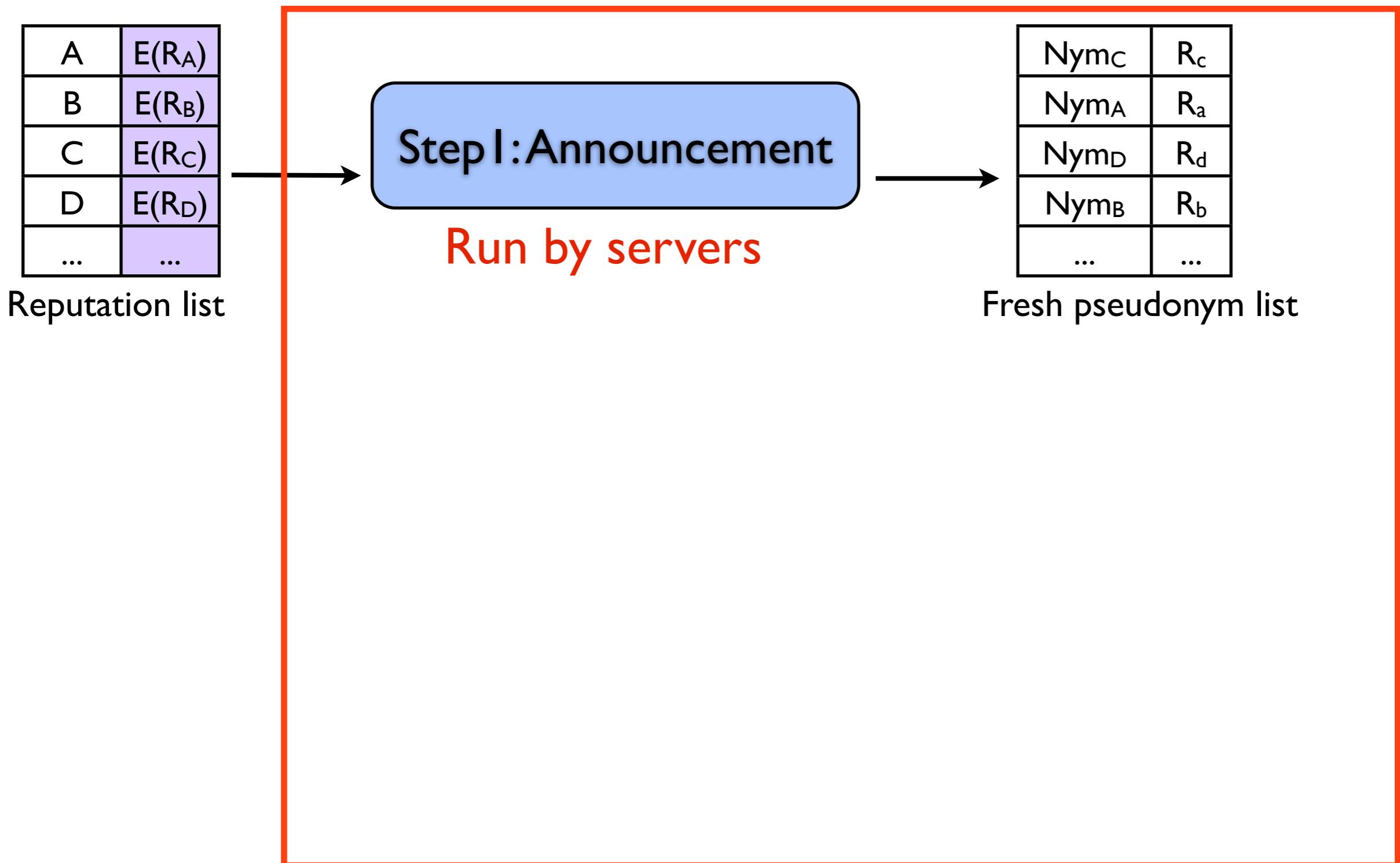
# Three Steps in Each Round

A	$E(R_A)$
B	$E(R_B)$
C	$E(R_C)$
D	$E(R_D)$
...	...

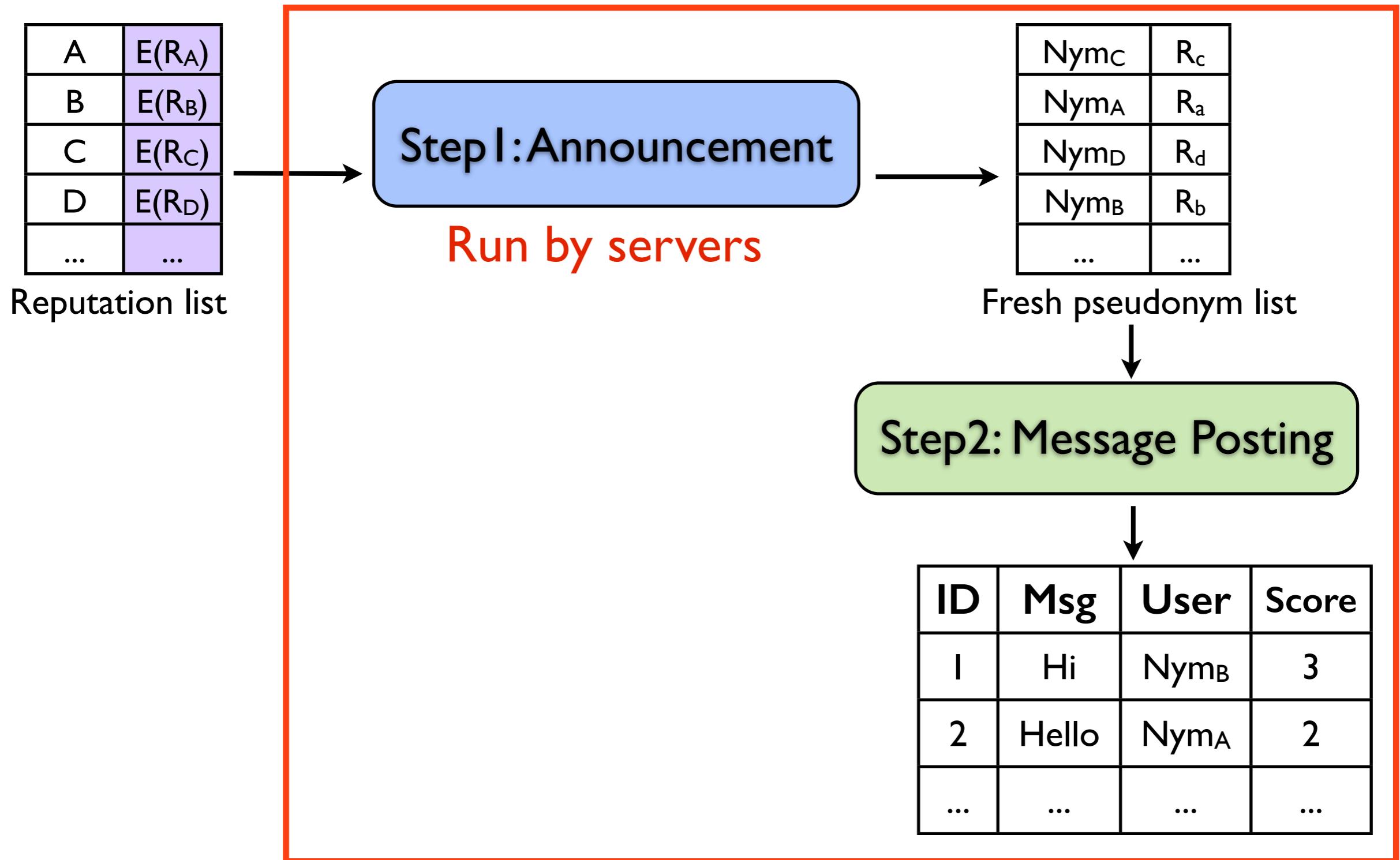
Reputation list



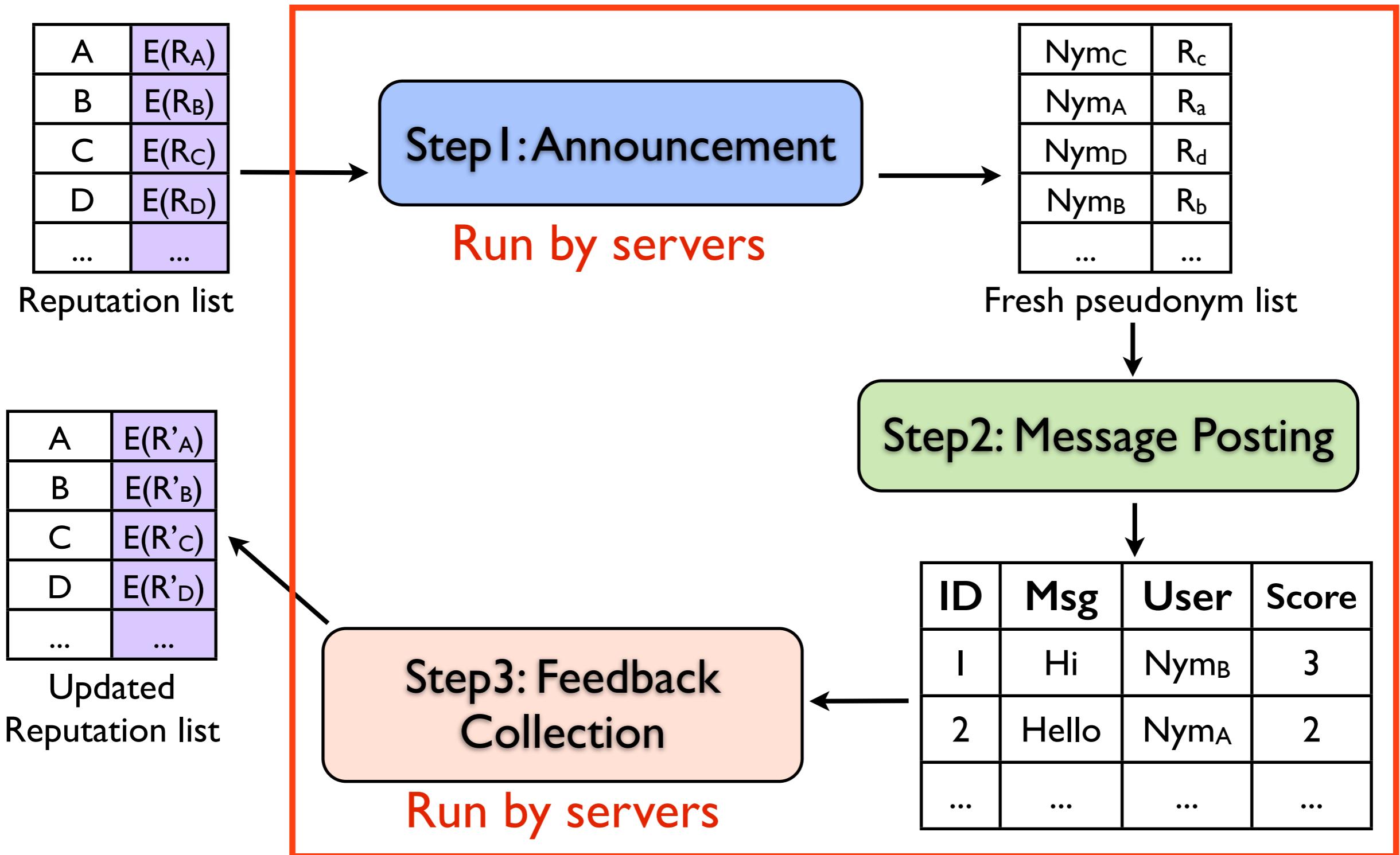
# Three Steps in Each Round



# Three Steps in Each Round

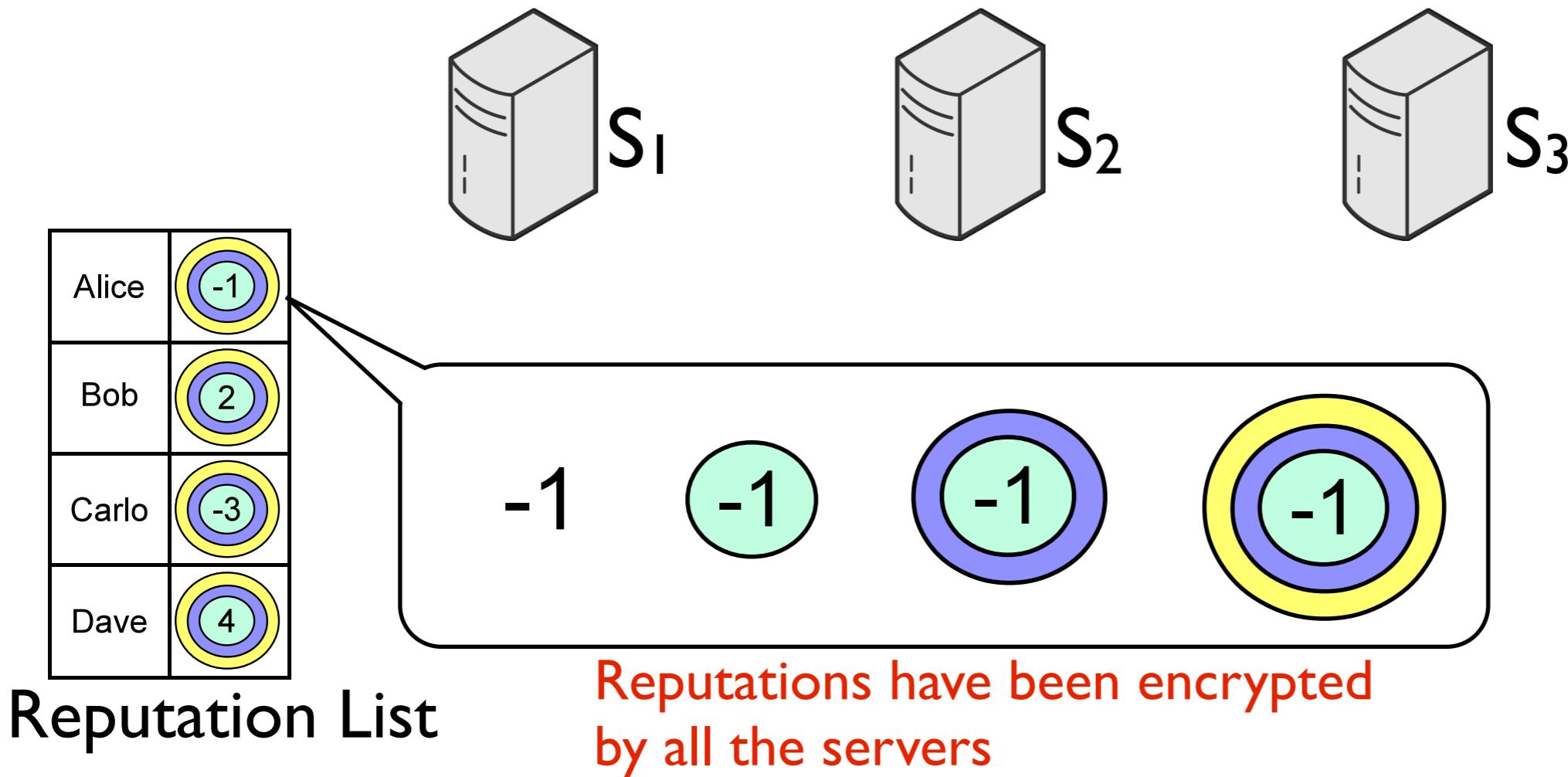


# Three Steps in Each Round

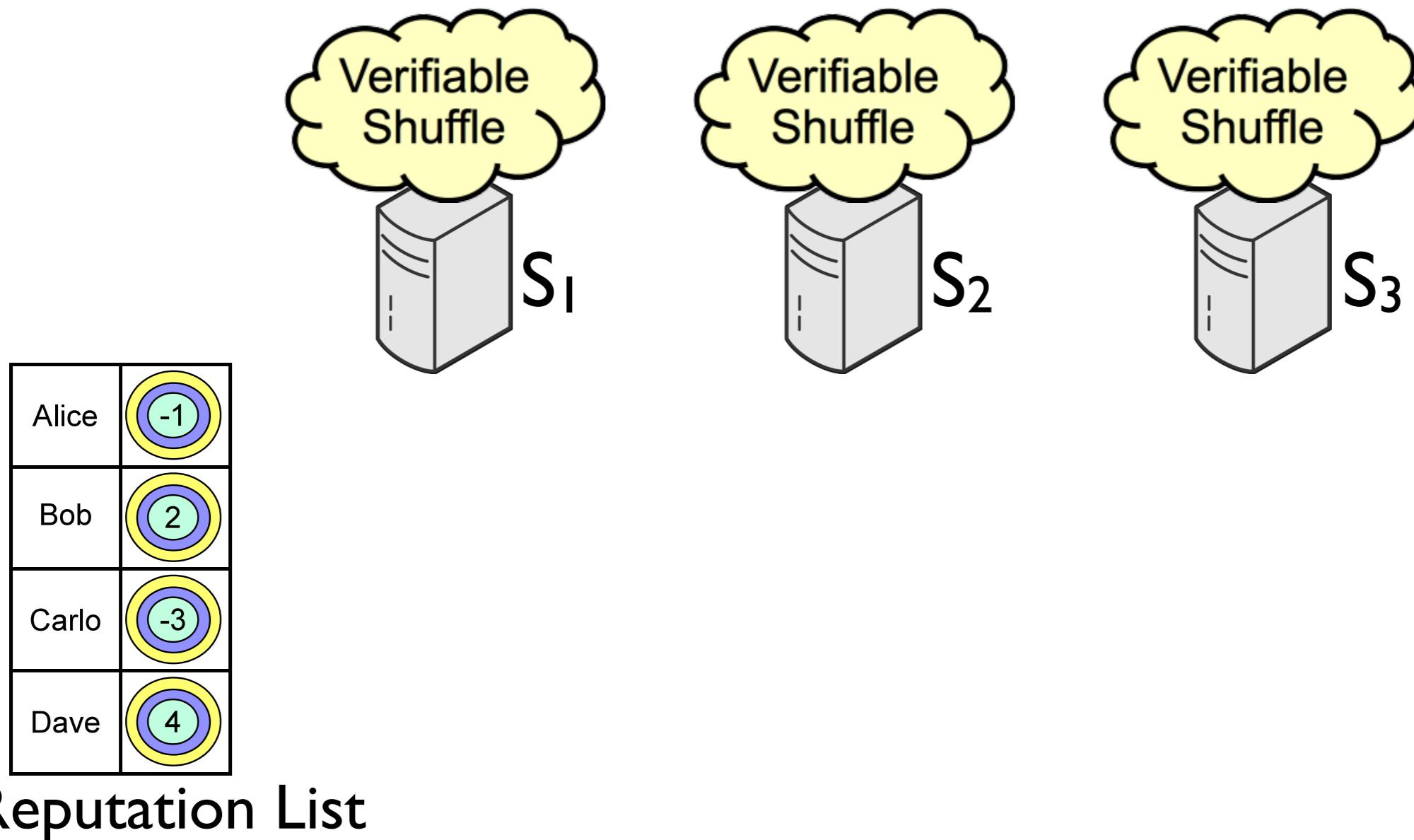


# Step 1: Announcement

# Step 1: Announcement

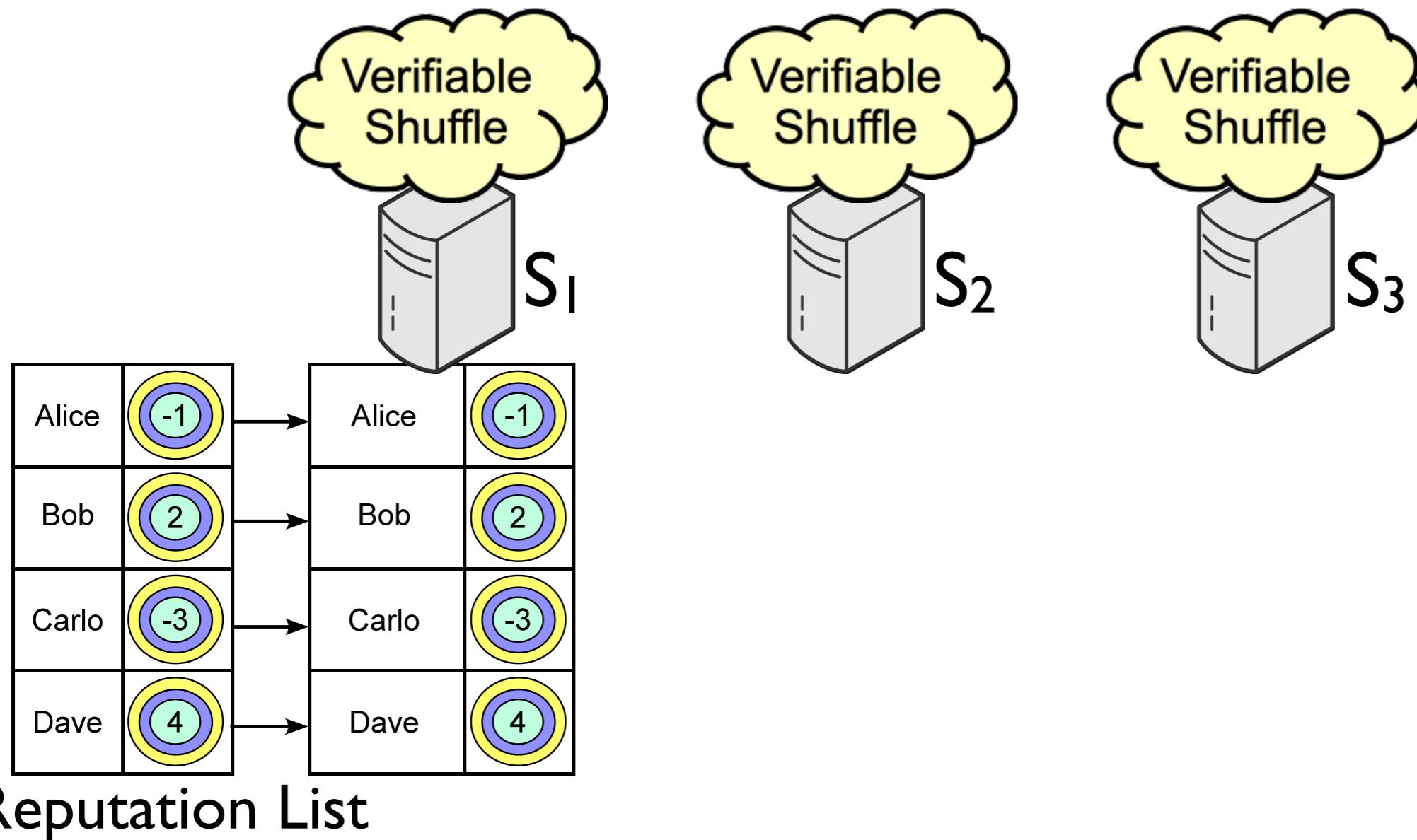


# Step 1: Announcement

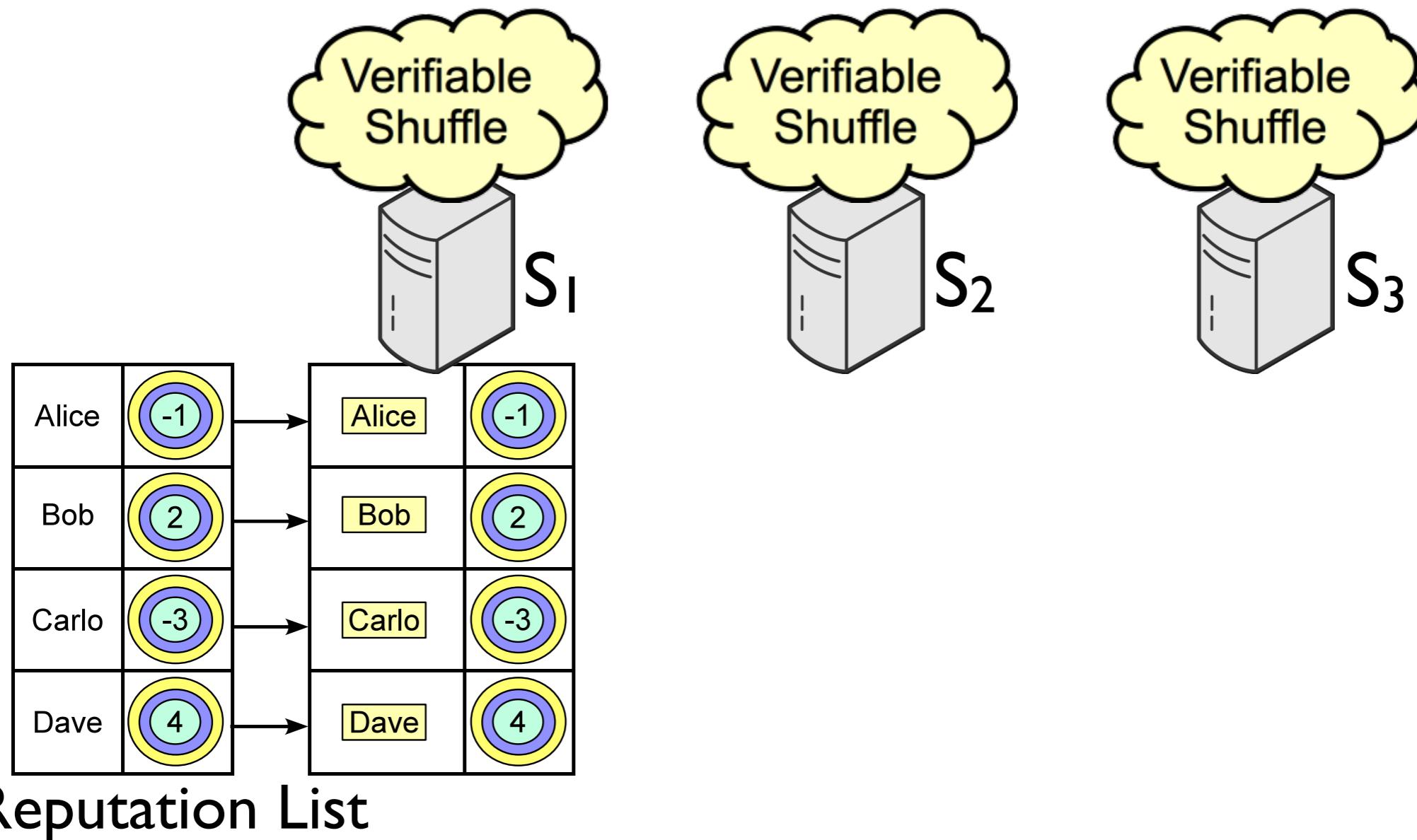


\* C. Andrew Neff. A verifiable secret shuffle and its application to e-voting. In CCS'01.

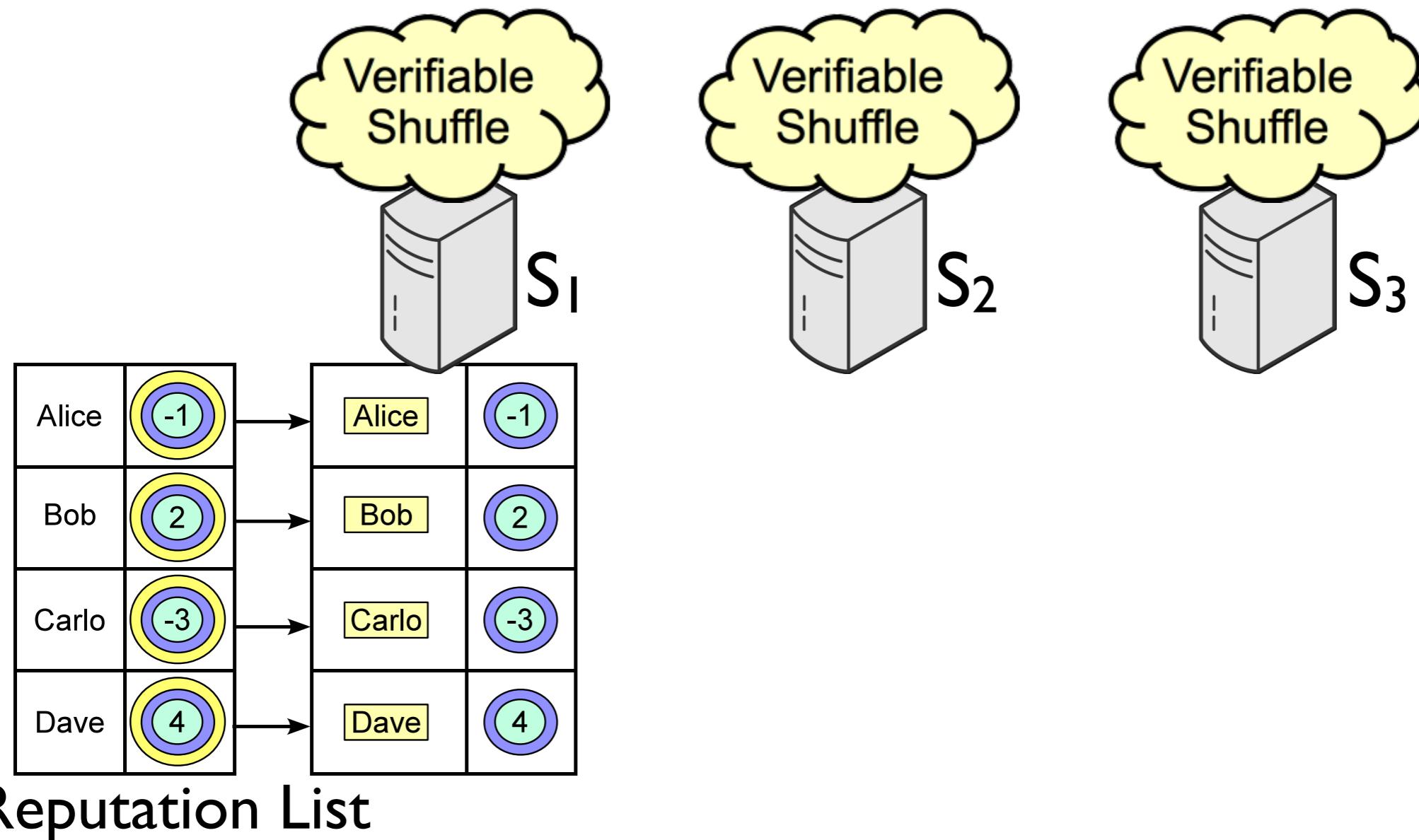
# Step 1: Announcement



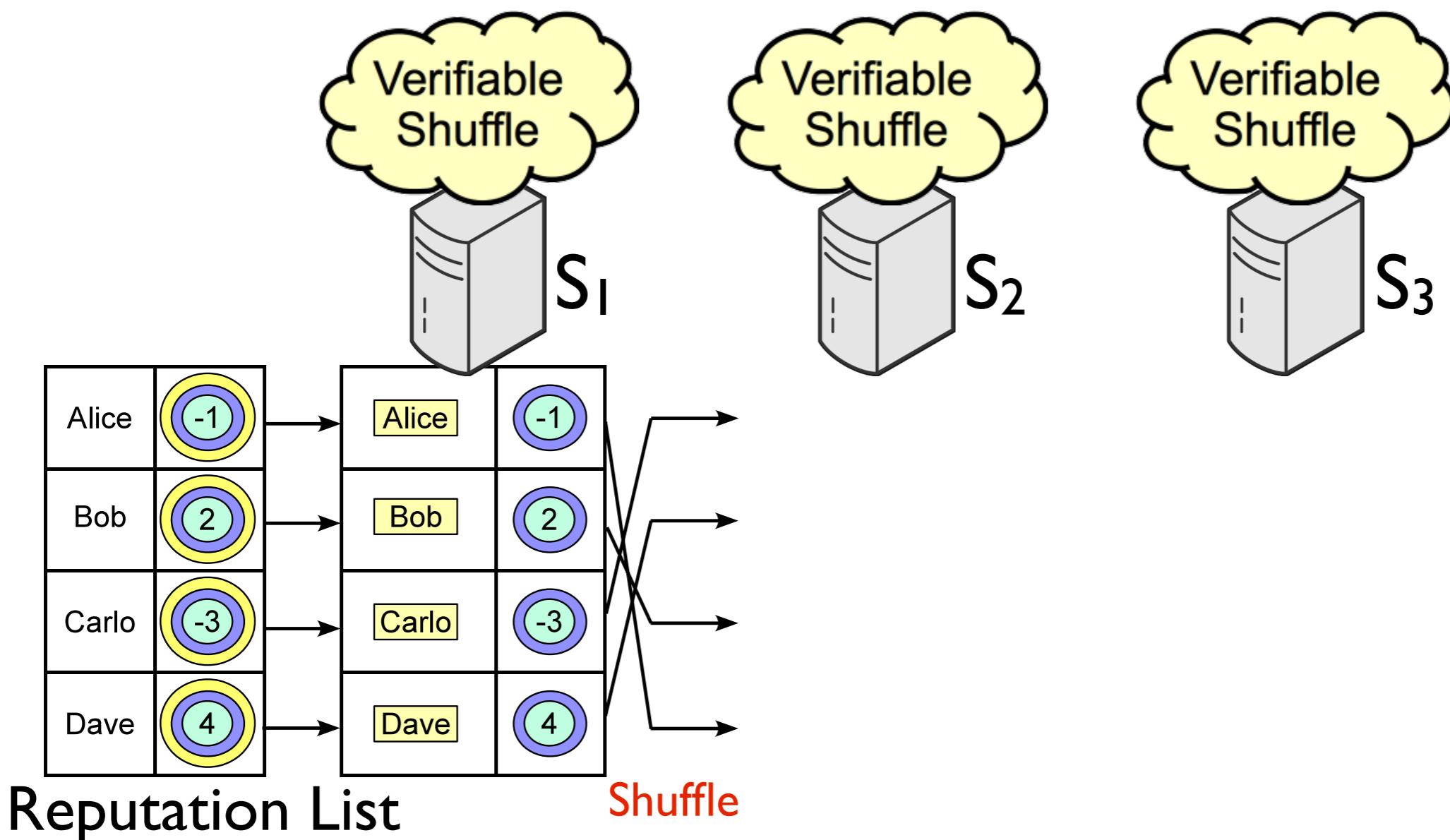
# Step 1: Announcement



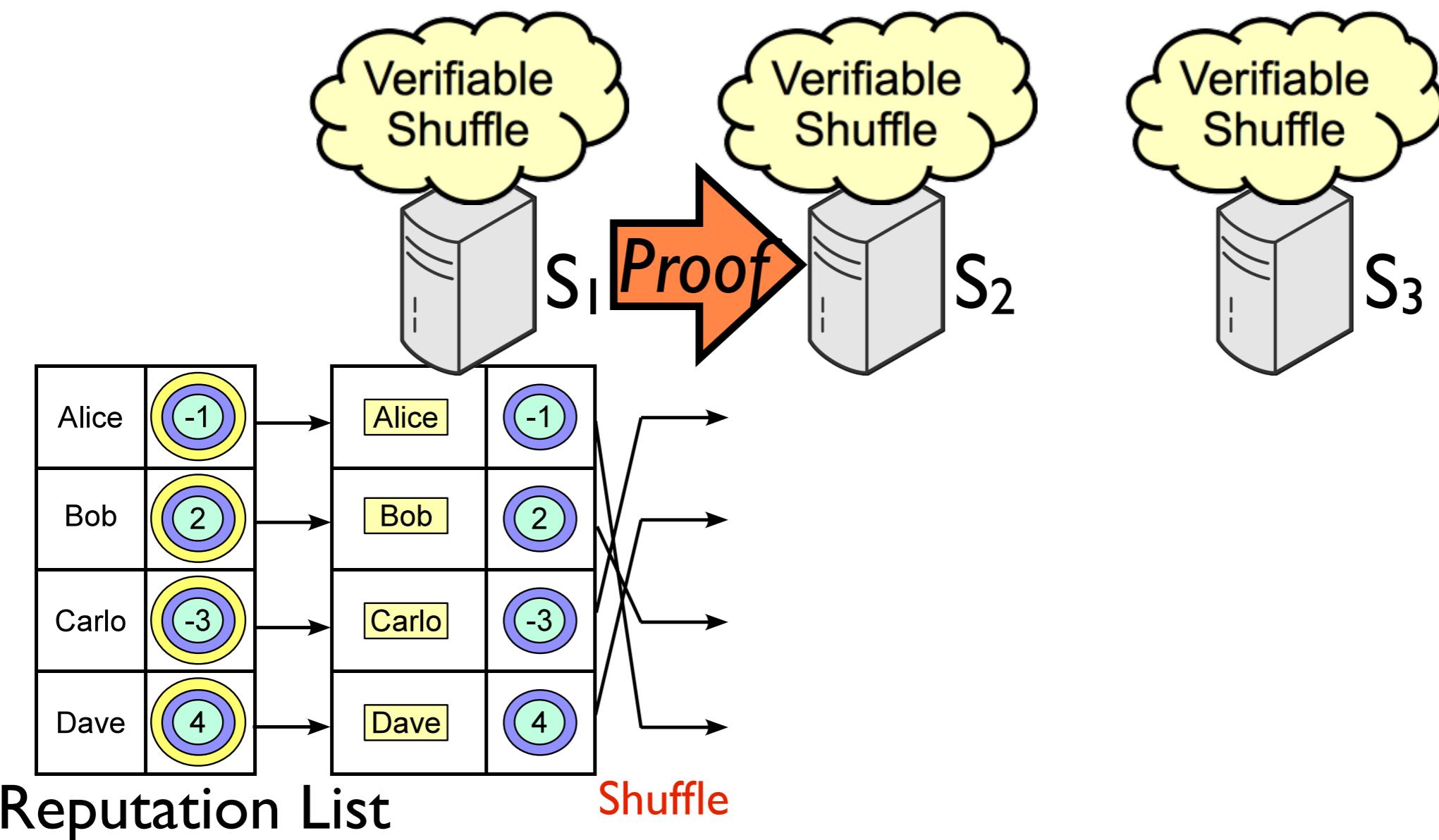
# Step 1: Announcement



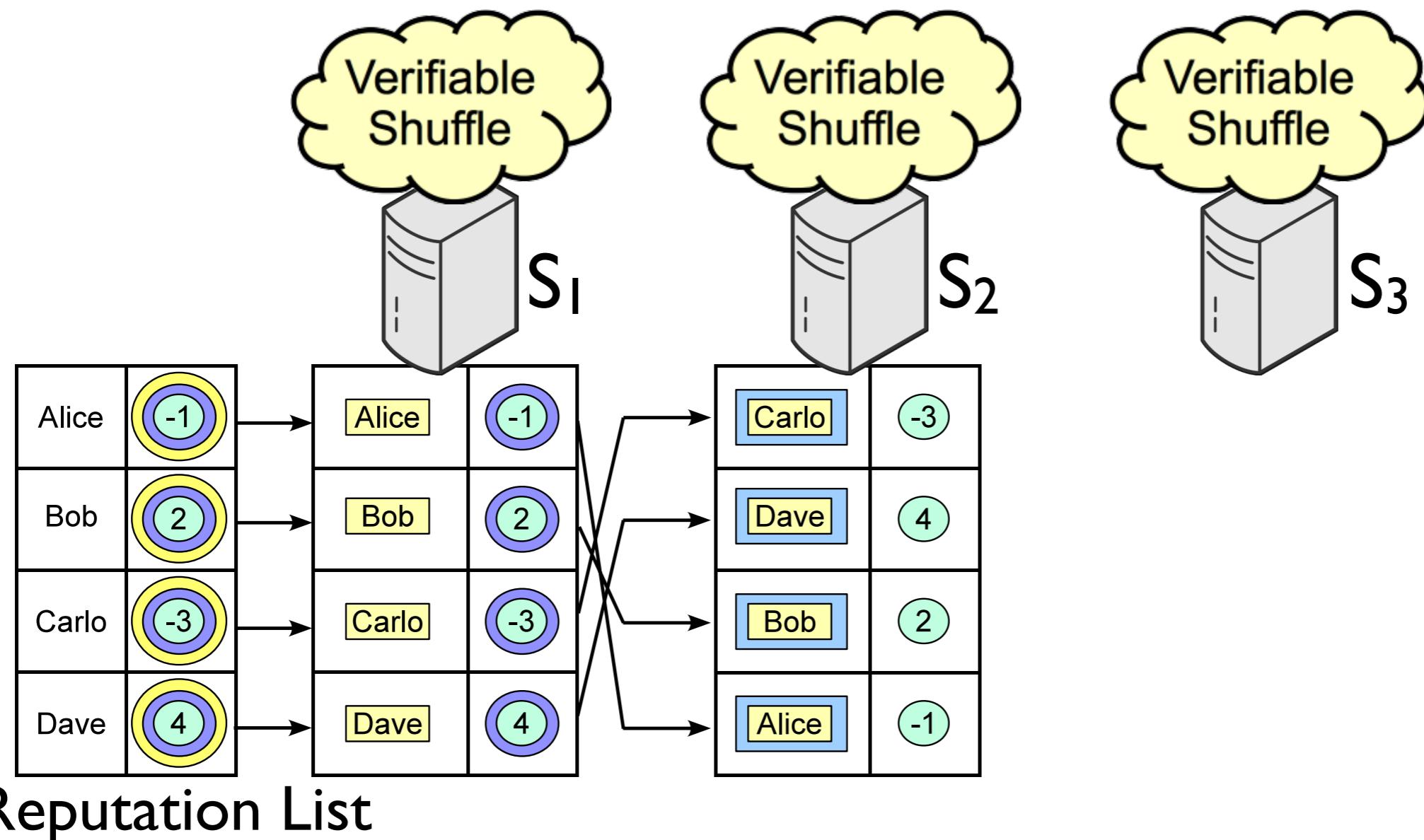
# Step 1: Announcement



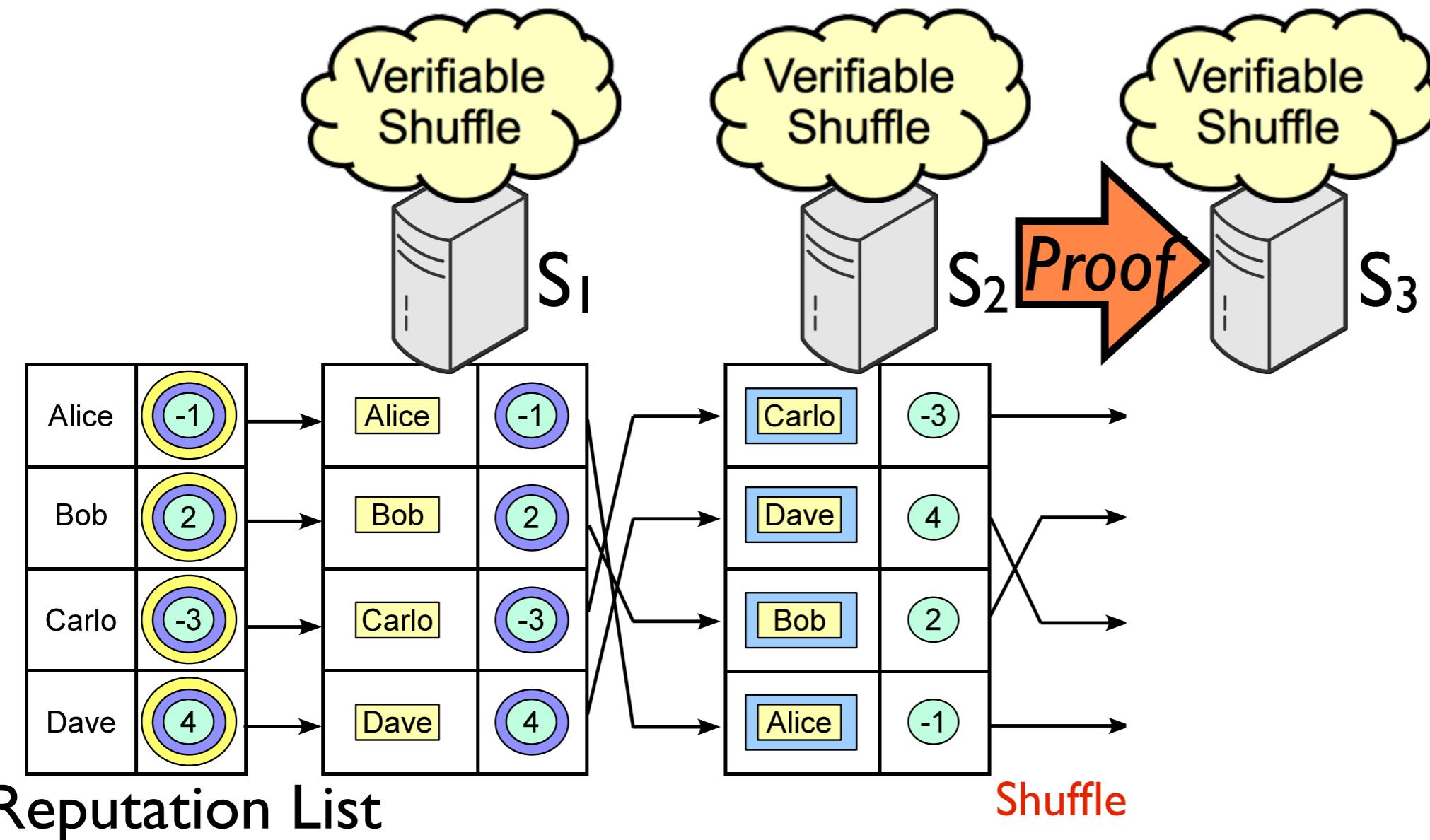
# Step 1: Announcement



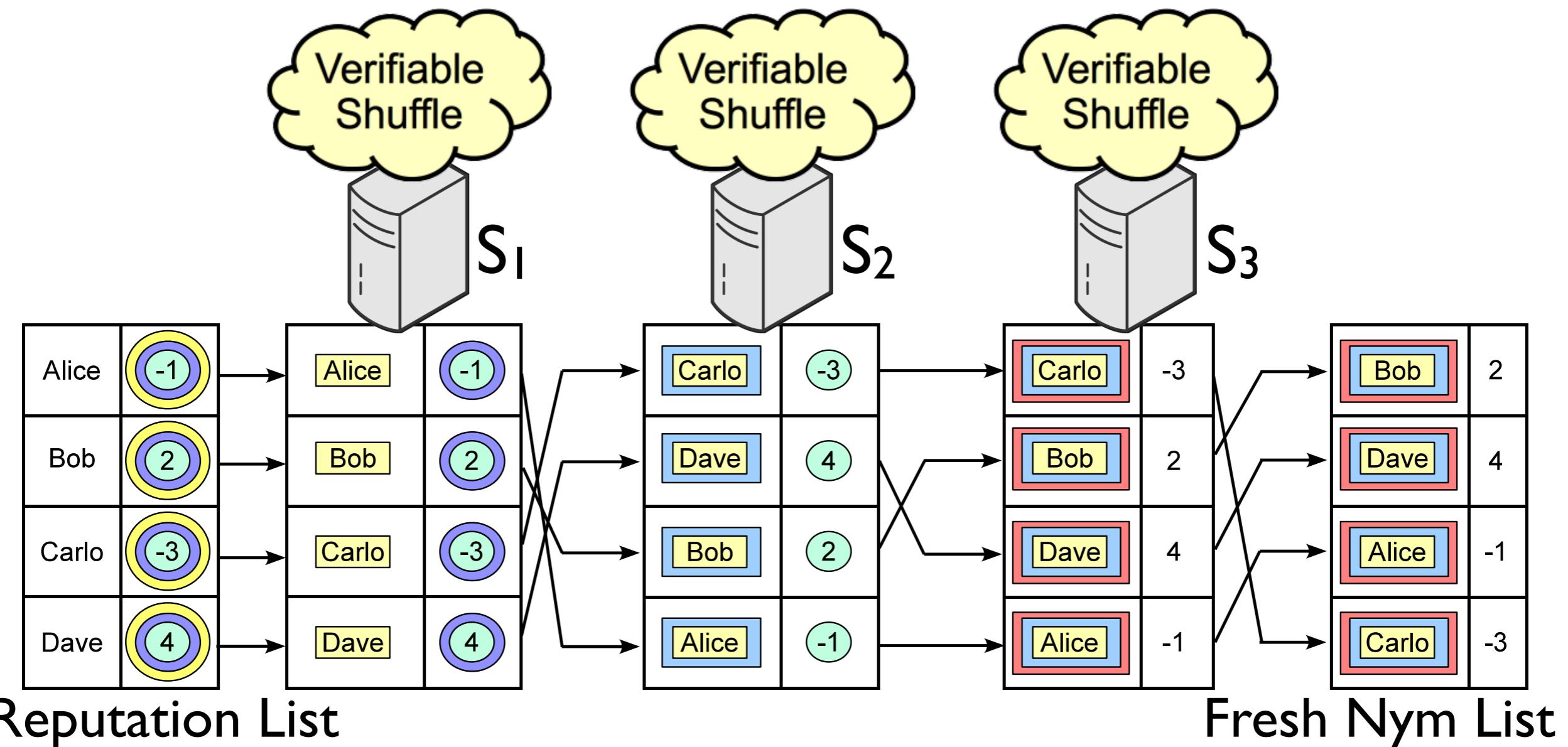
# Step 1: Announcement



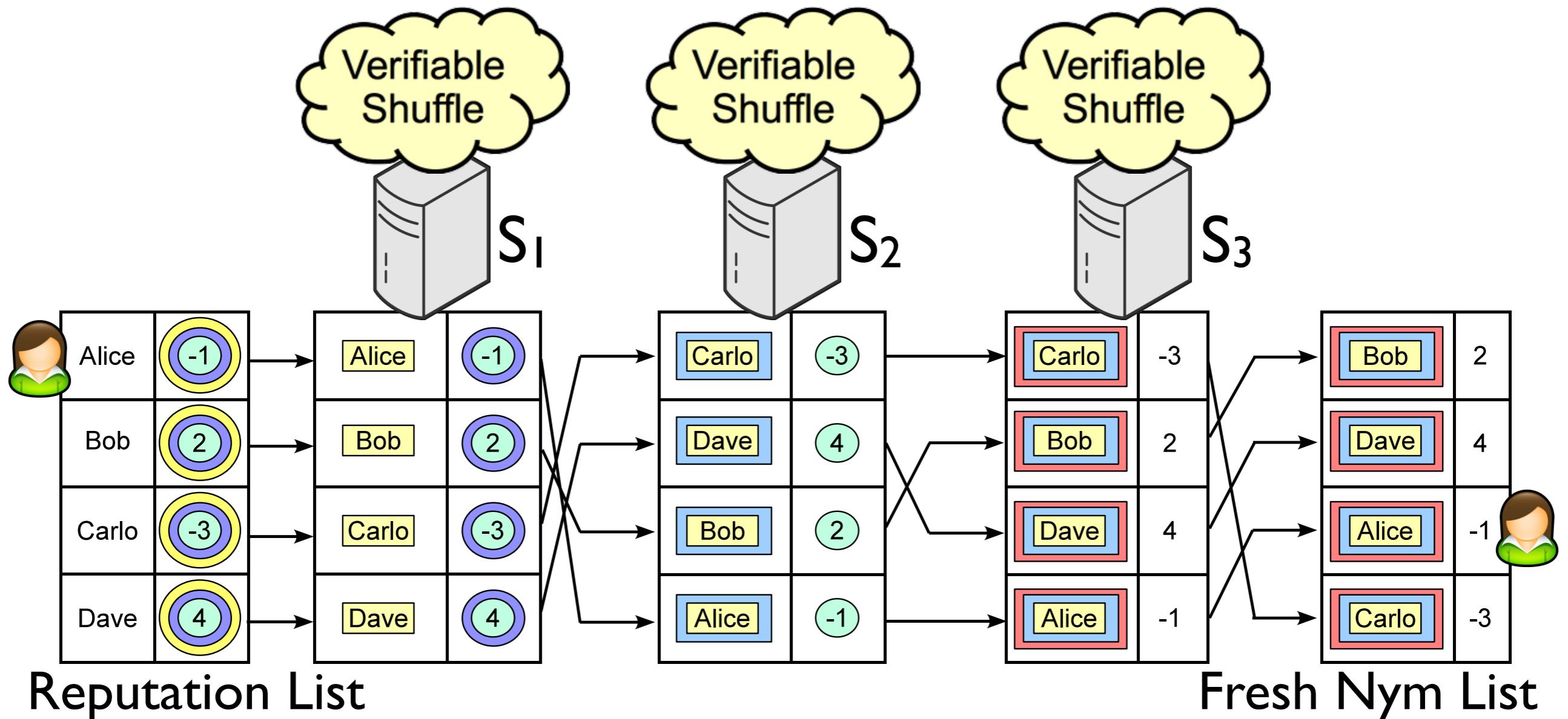
# Step 1: Announcement



# Step 1: Announcement



# Step 1: Announcement



# Step2: Message Posting

# Step2: Message Posting

Nym	Score
Nym <sub>C</sub>	-2
Nym <sub>A</sub>	2
Nym <sub>D</sub>	-1
Nym <sub>B</sub>	3
...	...

Fresh Nym List

# Step2: Message Posting

Nym	Score
Nym <sub>C</sub>	-2
Nym <sub>A</sub>	2
Nym <sub>D</sub>	-1
Nym <sub>B</sub>	3
...	...

Fresh Nym List

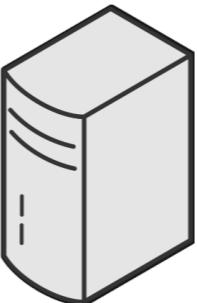
MsgID	Msg	User	Score
...	...	...	...

# Step2: Message Posting

Nym	Score
Nym <sub>C</sub>	-2
Nym <sub>A</sub>	2
Nym <sub>D</sub>	-1
Nym <sub>B</sub>	3
...	...



Bob



MsgID	Msg	User	Score
...	...	...	...

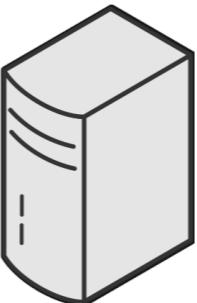
Fresh Nym List

# Step2: Message Posting

Nym	Score
Nym <sub>C</sub>	-2
Nym <sub>A</sub>	2
Nym <sub>D</sub>	-1
Nym <sub>B</sub>	3
...	...



Bob ("Hi", Nym<sub>B</sub>, Sig<sub>b</sub>)

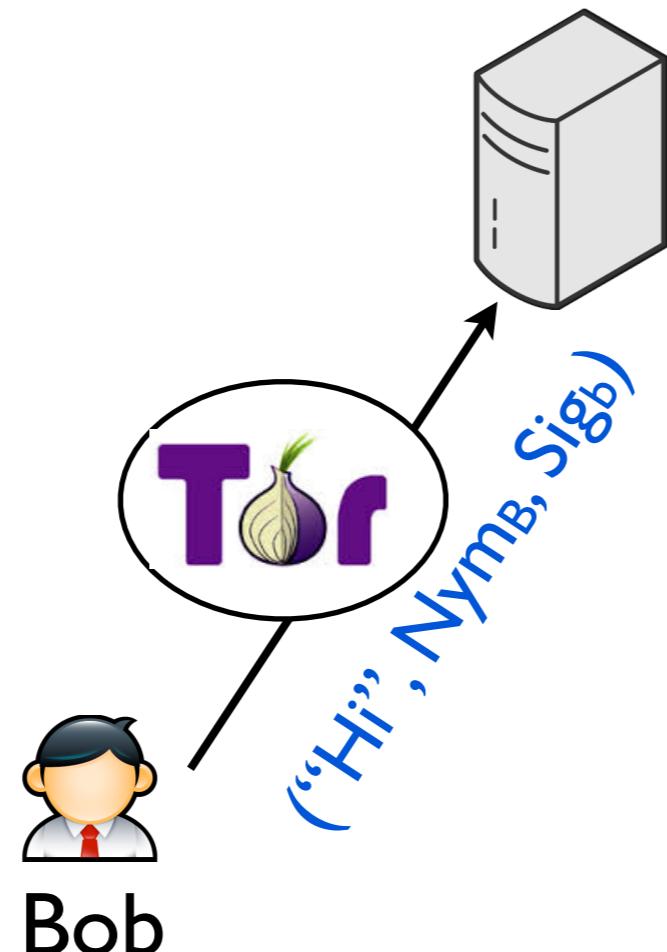


MsgID	Msg	User	Score
...	...	...	...

Fresh Nym List

# Step2: Message Posting

Nym	Score
Nym <sub>C</sub>	-2
Nym <sub>A</sub>	2
Nym <sub>D</sub>	-1
Nym <sub>B</sub>	3
...	...

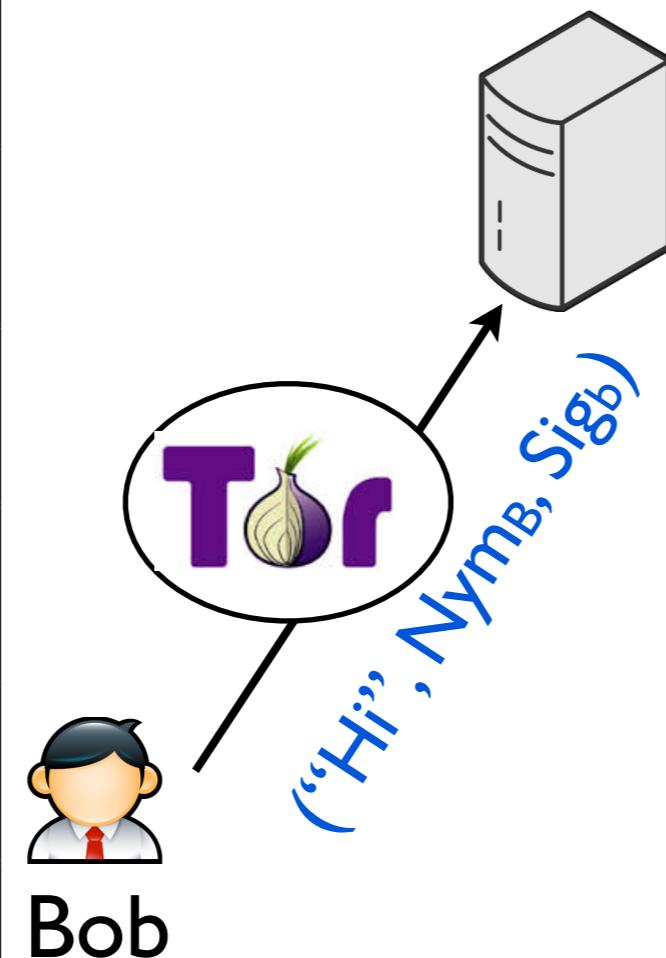


MsgID	Msg	User	Score
...	...	...	...

Fresh Nym List

# Step2: Message Posting

Nym	Score
Nym <sub>C</sub>	-2
Nym <sub>A</sub>	2
Nym <sub>D</sub>	-1
Nym <sub>B</sub>	3
...	...

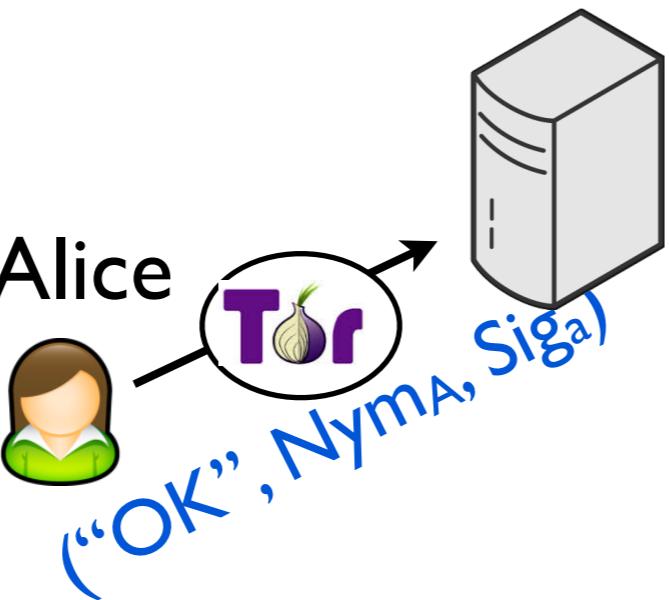


MsgID	Msg	User	Score
Msg1	Hi	Nym <sub>B</sub>	3
...	...	...	...
...	...	...	...

Fresh Nym List

# Step2: Message Posting

Nym	Score
Nym <sub>C</sub>	-2
Nym <sub>A</sub>	2
Nym <sub>D</sub>	-1
Nym <sub>B</sub>	3
...	...

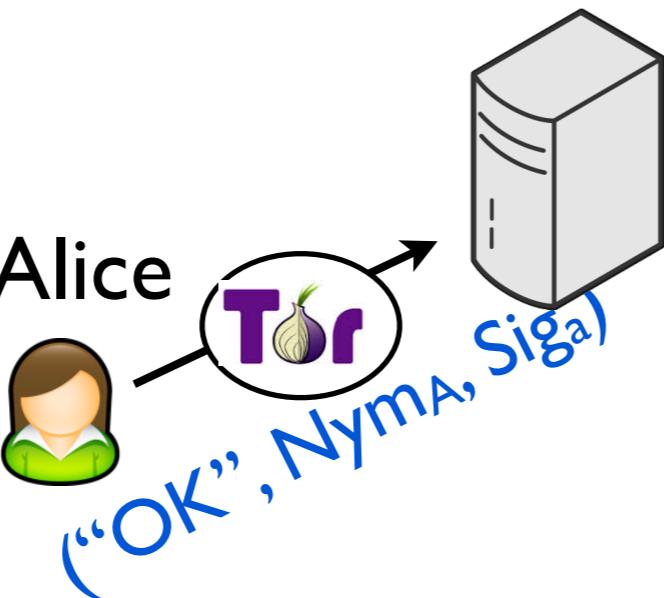


MsgID	Msg	User	Score
Msg1	Hi	Nym <sub>B</sub>	3
...	...	...	...

Fresh Nym List

# Step2: Message Posting

Nym	Score
Nym <sub>C</sub>	-2
Nym <sub>A</sub>	2
Nym <sub>D</sub>	-1
Nym <sub>B</sub>	3
...	...



MsgID	Msg	User	Score
Msg1	Hi	Nym <sub>B</sub>	3
Msg2	OK	Nym <sub>A</sub>	2
...	...	...	...

Fresh Nym List

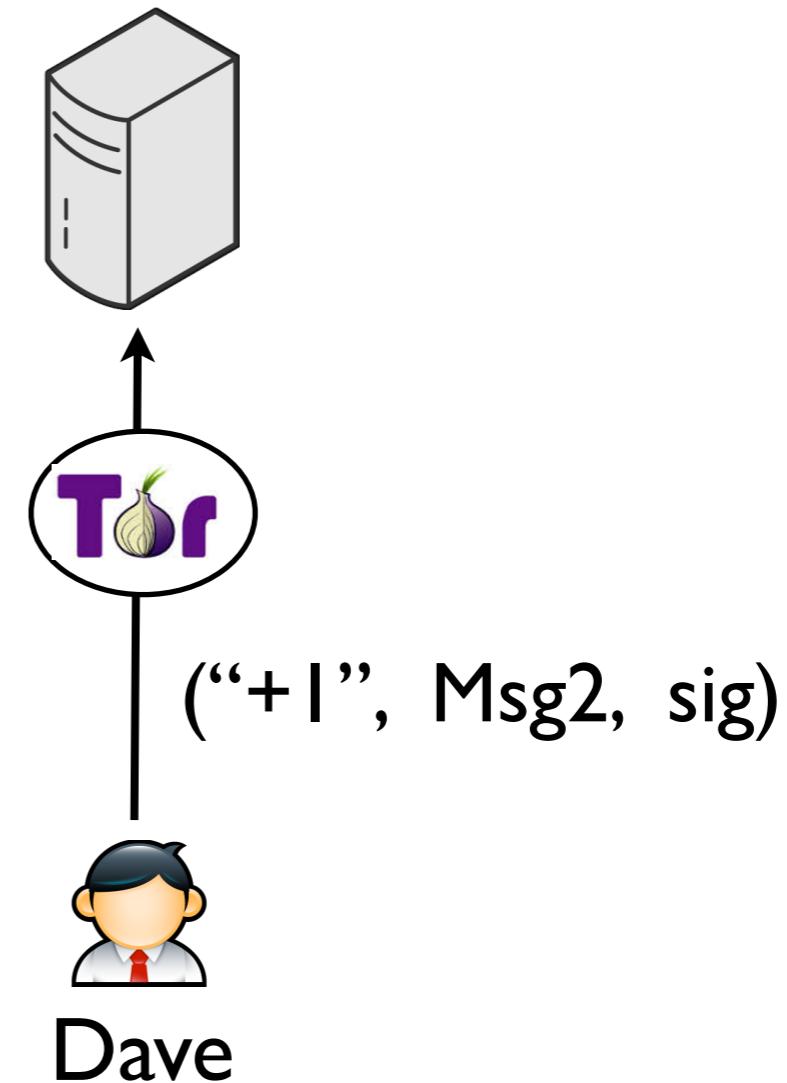
# Step3: Feedback Collection

# Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym <sub>B</sub>	3	
Msg2	Hello	Nym <sub>A</sub>	2	
...	...	...	...	

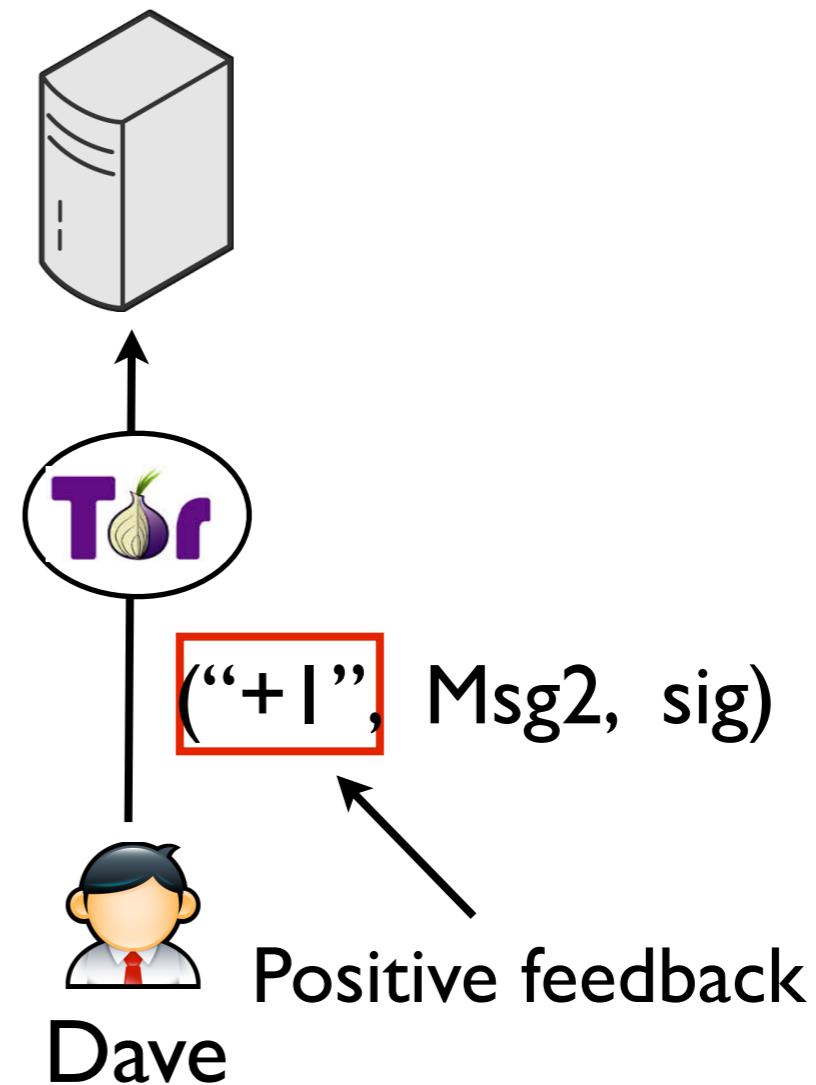
# Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym <sub>B</sub>	3	
Msg2	Hello	Nym <sub>A</sub>	2	
...	...	...	...	



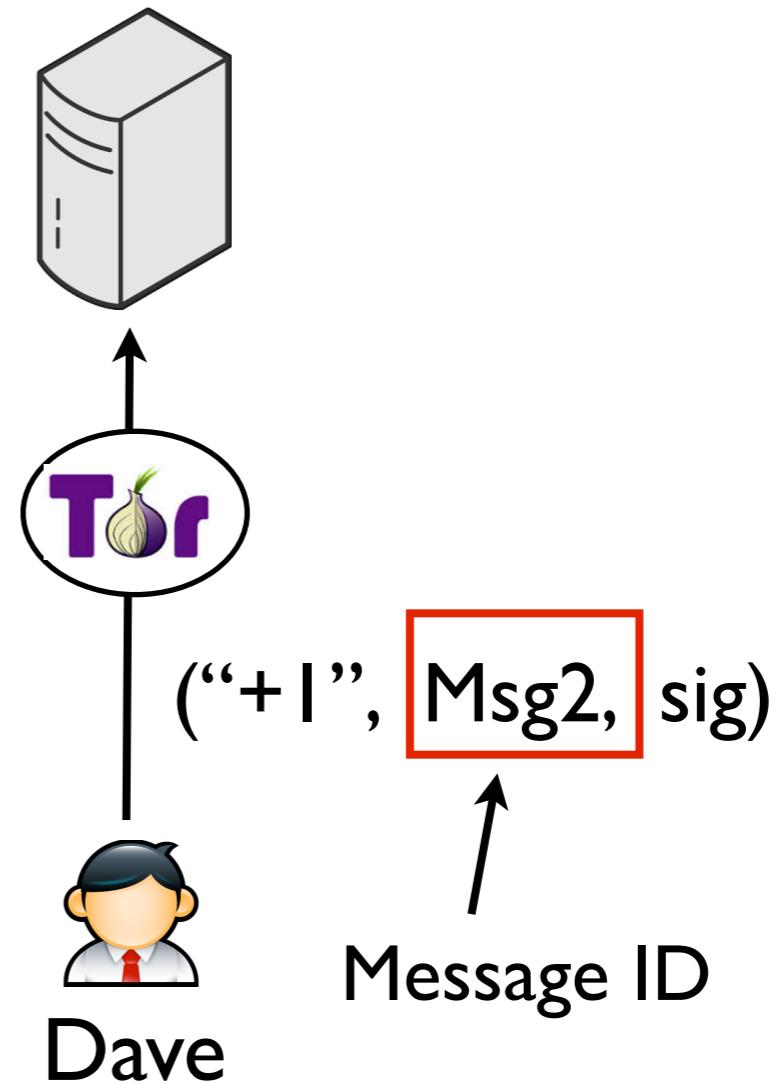
# Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym <sub>B</sub>	3	
Msg2	Hello	Nym <sub>A</sub>	2	
...	...	...	...	



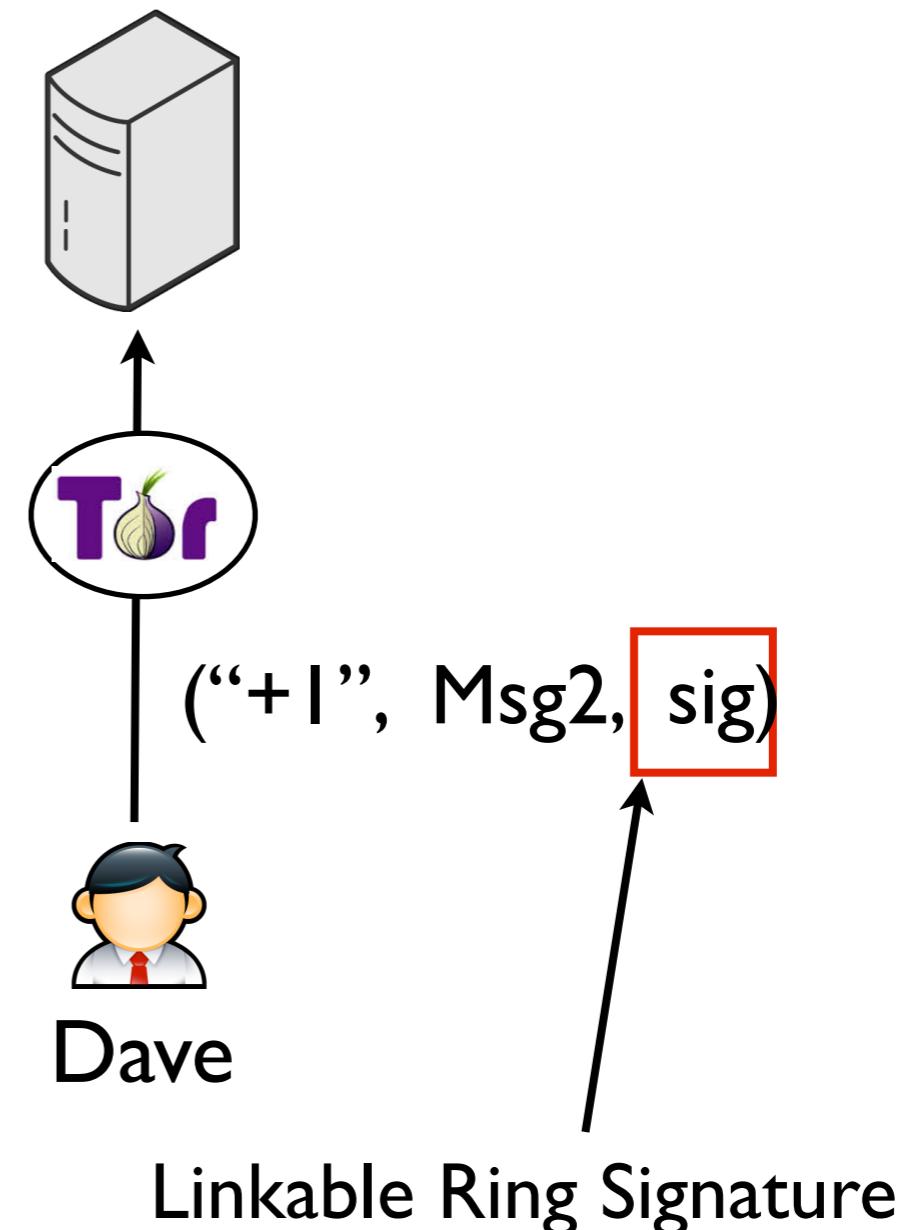
# Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym <sub>B</sub>	3	
Msg2	Hello	Nym <sub>A</sub>	2	
...	...	...	...	

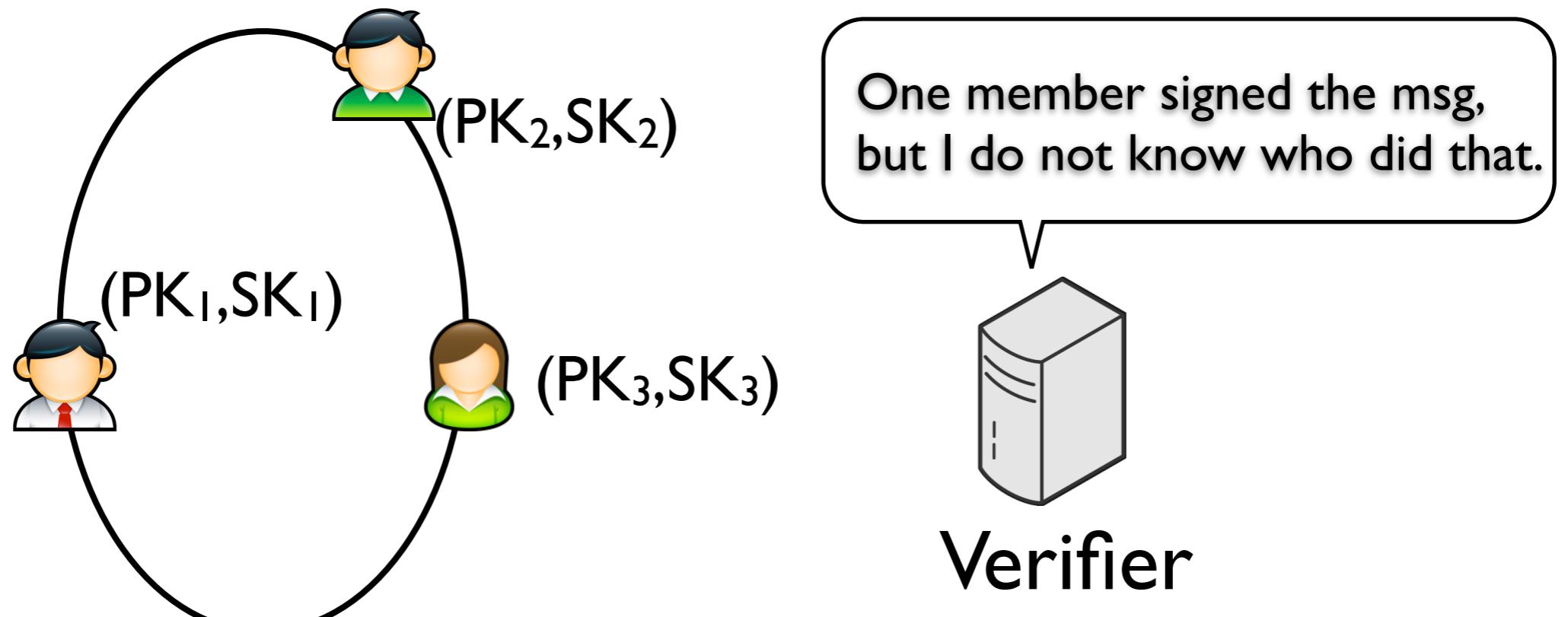


# Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym <sub>B</sub>	3	
Msg2	Hello	Nym <sub>A</sub>	2	
...	...	...	...	

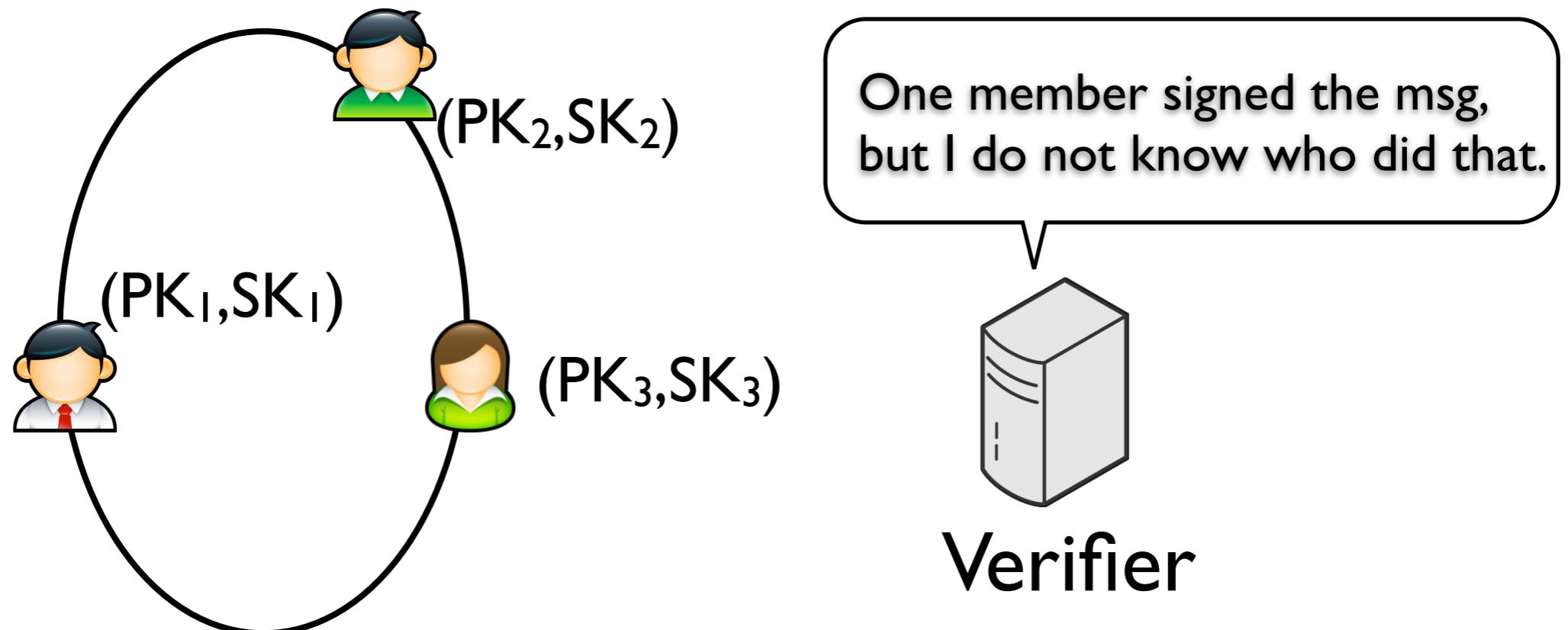


# Linkable Ring Signature (LRS)



\* Liu et al. Linkable ring signatures: Security models and new schemes. In ICCSA'05.

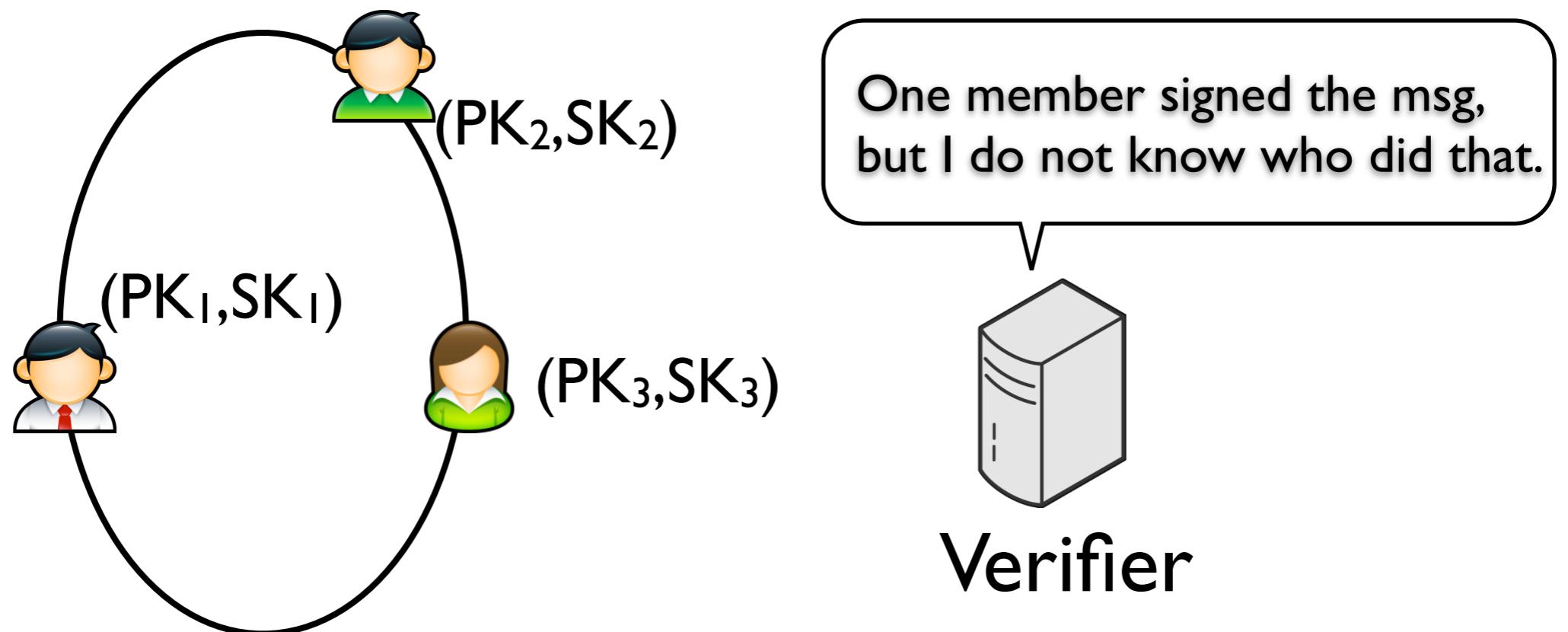
# Linkable Ring Signature (LRS)



- LRS can hide voter's pseudonym

\* Liu et al. Linkable ring signatures: Security models and new schemes. In ICCSA'05.

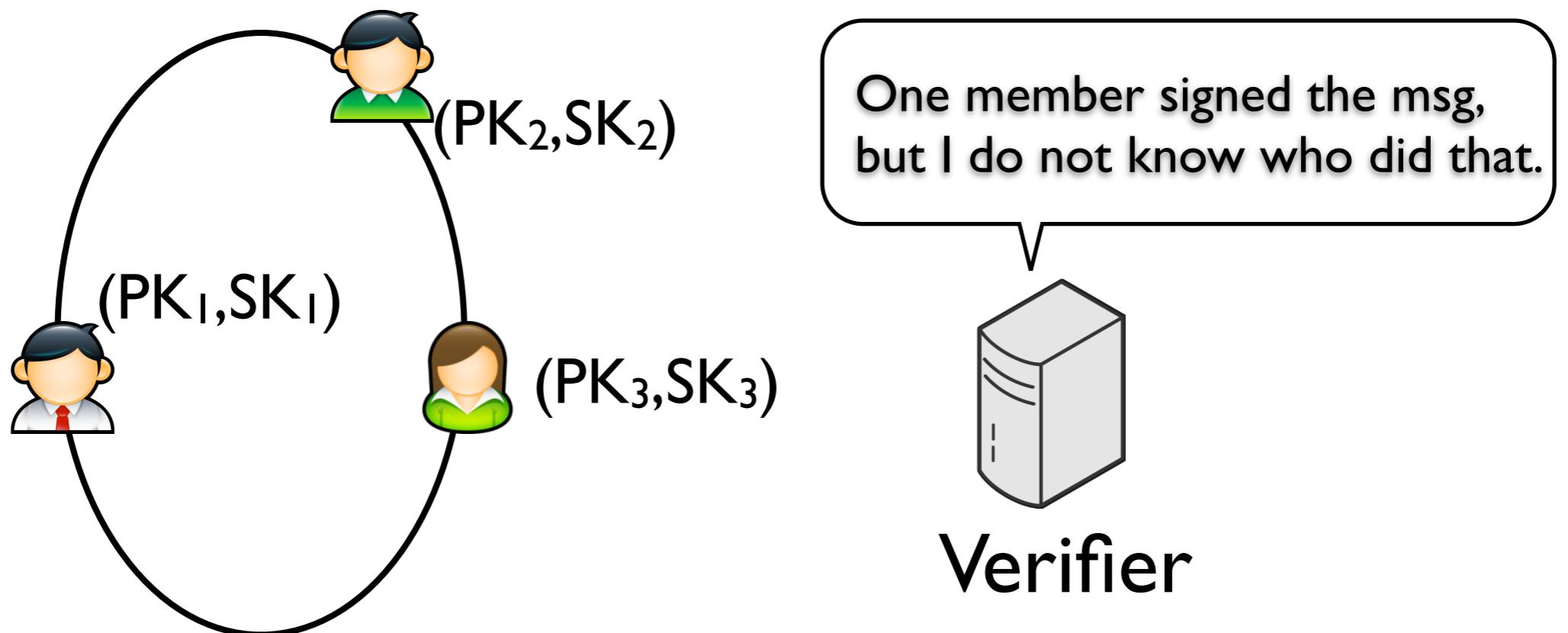
# Linkable Ring Signature (LRS)



- LRS can hide voter's pseudonym
- LRS can avoid duplicate votes

\* Liu et al. Linkable ring signatures: Security models and new schemes. In ICCSA'05.

# Linkable Ring Signature (LRS)



- LRS can hide voter's pseudonym
- LRS can avoid duplicate votes
- Different messages have different LRS

\* Liu et al. Linkable ring signatures: Security models and new schemes. In ICCSA'05.

# Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym <sub>B</sub>	3	<div style="display: flex; justify-content: space-around;"><div style="background-color: #ADD8E6; padding: 5px; border-radius: 10px;">Like: 2</div><div style="background-color: #FF4500; padding: 5px; border-radius: 10px;">Dislike: 1</div></div>
Msg2	Hello	Nym <sub>A</sub>	2	<div style="background-color: #ADD8E6; padding: 5px; border-radius: 10px;">Like: 1</div>
...	...	...	...	

# Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym <sub>B</sub>	3	<div style="display: flex; justify-content: space-around;"><div style="background-color: #ADD8E6; padding: 5px; border-radius: 10px;">Like: 2</div><div style="background-color: #FF4500; padding: 5px; border-radius: 10px;">Dislike: 1</div></div>
Msg2	Hello	Nym <sub>A</sub>	2	<div style="background-color: #ADD8E6; padding: 5px; border-radius: 10px;">Like: 1</div>
...	...	...	...	

AnonRep supports diverse reputation algorithms

# Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym <sub>B</sub>	3	<div style="display: flex; justify-content: space-between;"><div style="flex: 1; background-color: #e0f2ff; padding: 5px; border-radius: 10px;">Like: 2</div><div style="flex: 1; background-color: #ff7043; padding: 5px; border-radius: 10px;">Dislike: 1</div></div>
Msg2	Hello	Nym <sub>A</sub>	2	<div style="display: flex; justify-content: space-between;"><div style="flex: 1; background-color: #e0f2ff; padding: 5px; border-radius: 10px;">Like: 1</div><div style="flex: 1;"></div></div>
...	...	...	...	

$$3 + 2 - 1 = 4$$

$$2 + 1 = 3$$

# Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym <sub>B</sub>	4	Like: 2 Dislike: 1
Msg2	Hello	Nym <sub>A</sub>	3	Like: 1
...	...	...	...	

$$3+2-1=4$$

$$2+1=3$$

Nym<sub>B</sub>'s reputation becomes 4  
Nym<sub>A</sub>'s reputation becomes 3

# Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym <sub>B</sub>	4	Like: 2 Dislike: 1
Msg2	Hello	Nym <sub>A</sub>	3	Like: 1
...	...	...	...	

$$3+2-1=4$$

$$2+1=3$$

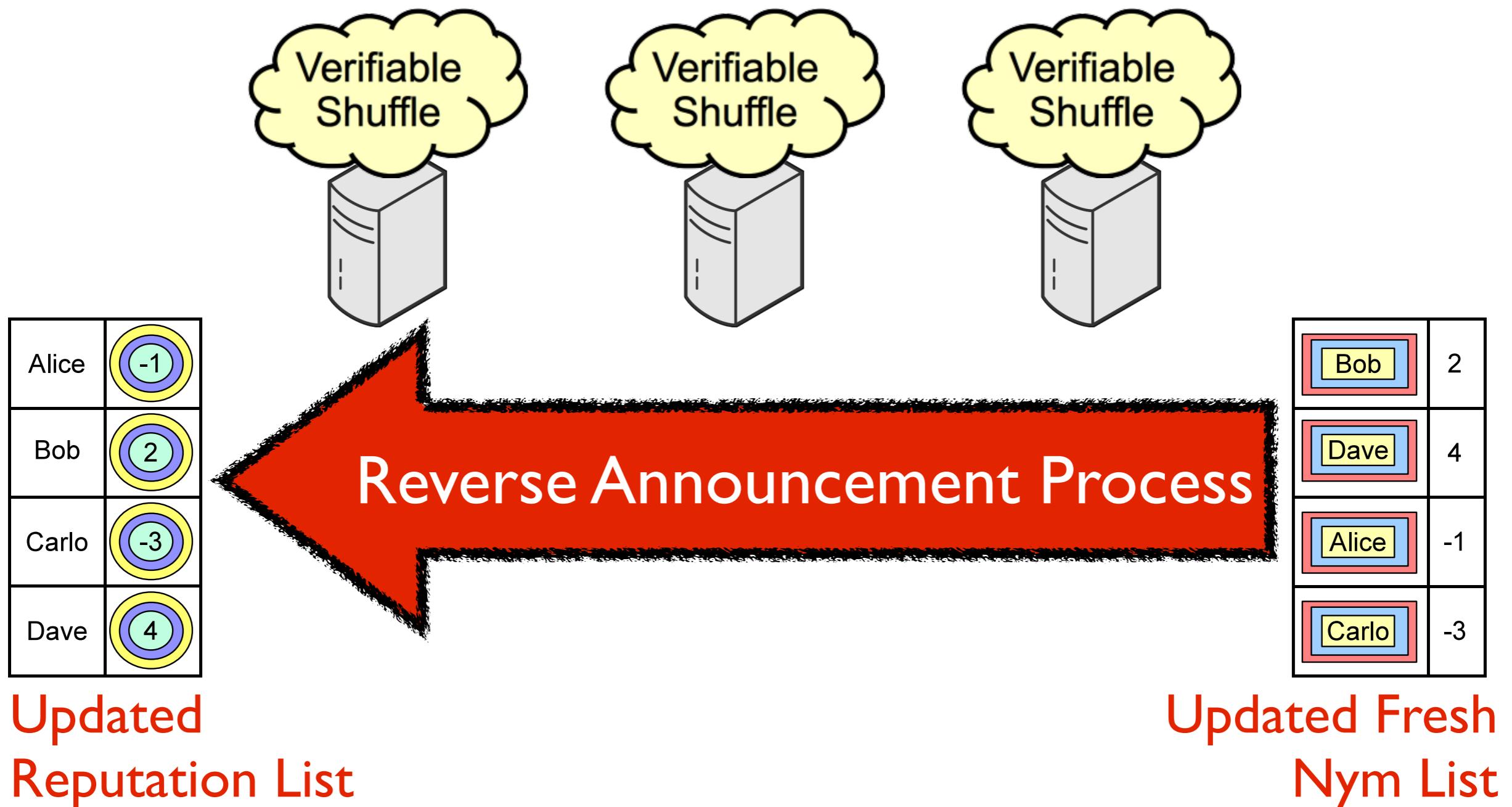
Fresh Nym list with updated reputation

# Step3: Feedback Collection

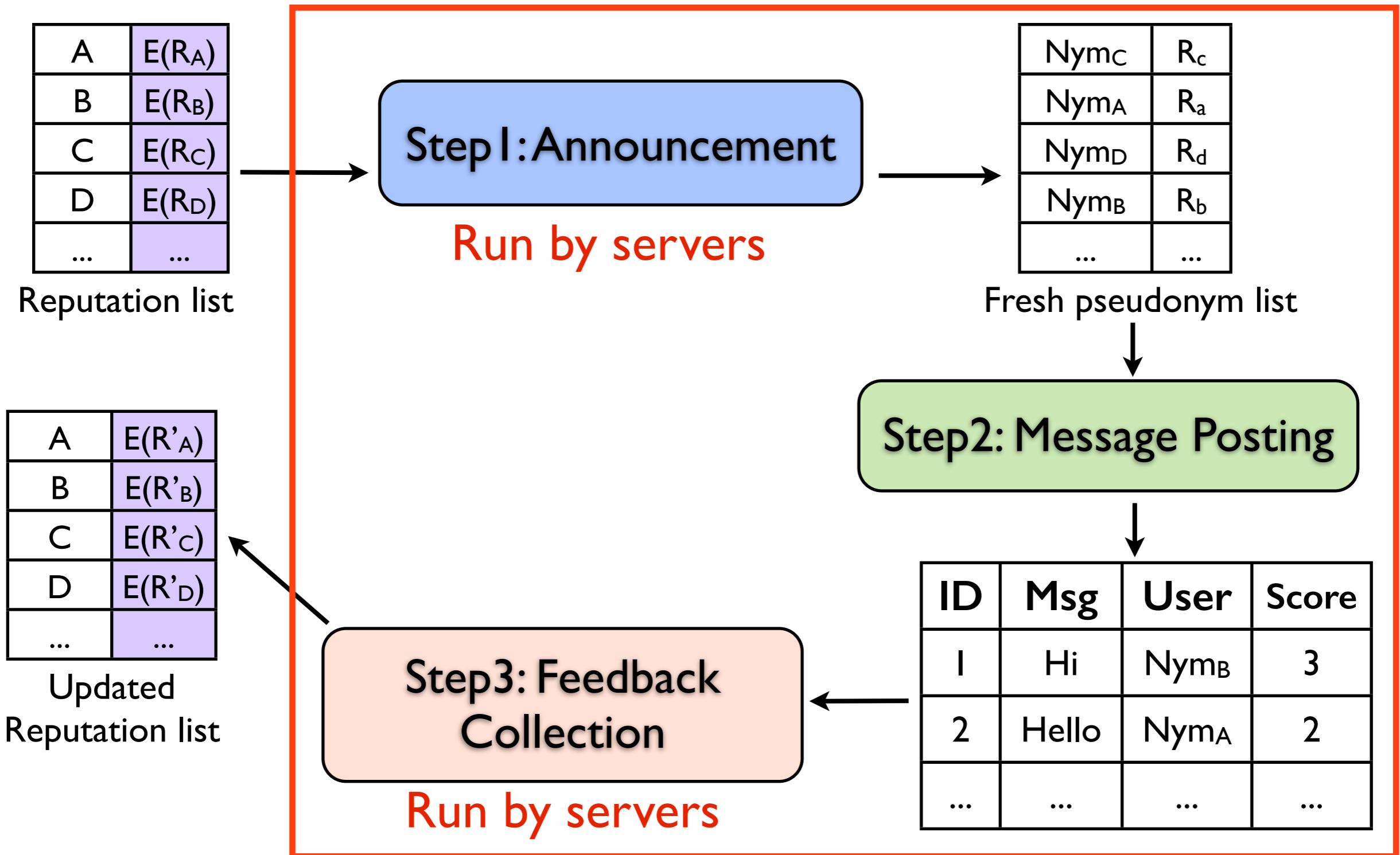
Bob	2
Dave	4
Alice	-1
Carlo	-3

Updated Fresh  
Nym List

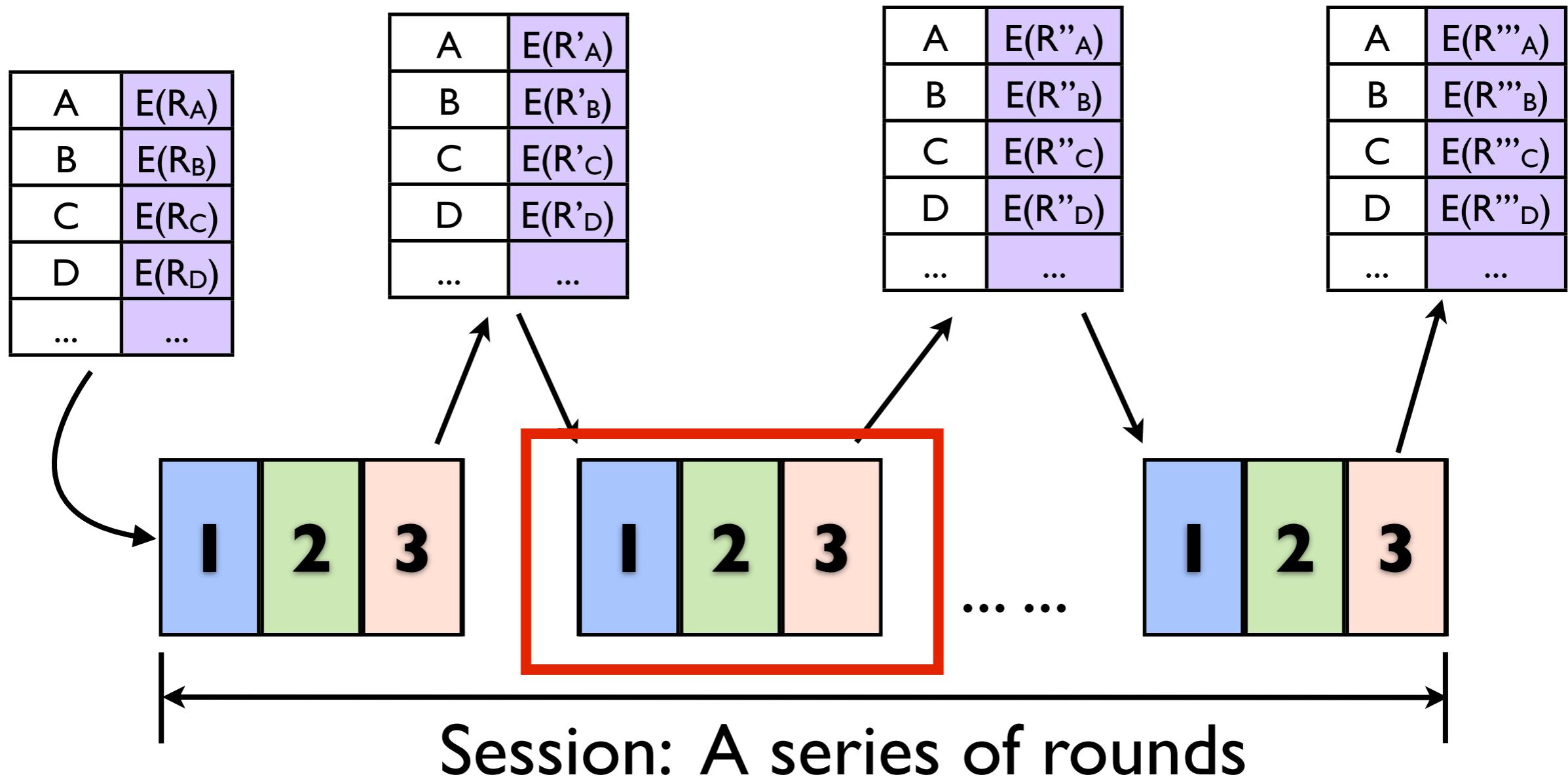
# Step3: Feedback Collection



# Three Steps in Each Round

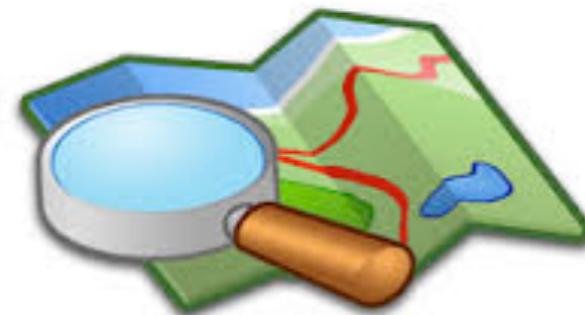


# Session, Rounds and Steps



# Road-Map

- Motivations
- AnonRep Design
- Practical Considerations
- Evaluation



# Practical Considerations

- Intersection attacks on special reputations
- Performance optimization
- Misbehavior detection
- Registration verification

# Practical Considerations

- Intersection attacks on special reputations
- Performance optimization
- Misbehavior detection
- Registration verification

Please see our paper for more details

# Intersection Attack

Msg1	csdfsa(100)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	.... ....	...

Round  $i$

# Intersection Attack

Msg1	csdfsa(100)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	.... ....	...

Round  $i$

# Intersection Attack

Msg1	csdfsa(100)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	.... ....	...

Round  $i$

Msg4	u78edja(-2)	like:0 dislike:2
Msg5	79fdad(4)	like:6 dislike:3
Msg6	ie821a(101)	like:0 dislike:1
...	.... ....	...

Round  $i+1$

# Intersection Attack

Msg1	csdfsa(100)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	.... ....	...

Round  $i$

Msg4	u78edja(-2)	like:0 dislike:2
Msg5	79fdad(4)	like:6 dislike:3
Msg6	ie821a(101)	like:0 dislike:1
...	.... ....	...

Round  $i+1$

# Intersection Attack

Msg1	csdfsa(100)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	.... ....	...

Round  $i$

Msg4	u78edja(-2)	like:0 dislike:2
Msg5	79fdad(4)	like:6 dislike:3
Msg6	ie821a(101)	like:0 dislike:1
...	.... ....	...

Round  $i+1$

Msg7	829q(-2)	like:1 dislike:1
Msg8	fapqx(100)	like:3 dislike:2
Msg9	zcvbfa(2)	like:1 dislike:2
...	.... ....	...

Round  $i+2$

# Intersection Attack

Msg1	csdfsa(100)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	.... ....	...

Round  $i$

Msg4	u78edja(-2)	like:0 dislike:2
Msg5	79fdad(4)	like:6 dislike:3
Msg6	ie821a(101)	like:0 dislike:1
...	.... ....	...

Round  $i+1$

Msg7	829q(-2)	like:1 dislike:1
Msg8	fapqx(100)	like:3 dislike:2
Msg9	zcvbfa(2)	like:1 dislike:2
...	.... ....	...

Round  $i+2$

# Intersection Attack

Msg1	csdfsa(100)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	.... ....	...

Round  $i$

Msg4	u78edja(-2)	like:0 dislike:2
Msg5	79fdad(4)	like:6 dislike:3
Msg6	ie821a(101)	like:0 dislike:1
...	.... ....	...

Round  $i+1$

Msg7	829q(-2)	like:1 dislike:1
Msg8	fapqx(100)	like:3 dislike:2
Msg9	zcvbfa(2)	like:1 dislike:2
...	.... ....	...

Round  $i+2$

# Security-Enhanced AnonRep

# Security-Enhanced AnonRep

- Actual reputation scores are maintained as ciphertexts
- Solution: Homomorphic encryption [1]

[1] Cramer et al. A secure and optimally efficient multi-authority election scheme. In EUROCRYPT'97.

# Security-Enhanced AnonRep

- Actual reputation scores are maintained as ciphertexts
- Solution: Homomorphic encryption [1]
  
- Reputation budget: posting message with budget < actual score
- Solution: Zero-knowledge proof [2]

[1] Cramer et al. A secure and optimally efficient multi-authority election scheme. In EUROCRYPT'97.

[2] Camenisch et al. Proof systems for general statements about discrete logarithms. In ETH TR'97.

# Security-Enhanced AnonRep

Round <i>i</i>	Round <i>i+1</i>	Round <i>i+2</i>
Msg1 csdfsa(2) like:1 dislike:0	Msg4 u78edja(-2) like:0 dislike:2	Msg7 829q(-2) like:1 dislike:1
Msg2 9sf1aaa(2) like:1 dislike:4	Msg5 79fdad(4) like:6 dislike:3	Msg8 fapqx(1) like:3 dislike:2
Msg3 ty4azko(3) like:3 dislike:4	Msg6 ie821a(5) like:0 dislike:1	Msg9 zcvbfa(2) like:1 dislike:2
... ....	... ....	... ....

# Security-Enhanced AnonRep

Msg1	csdfsa(2)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	.... ....	...

Round  $i$

Msg4	u78edja(-2)	like:0 dislike:2
Msg5	79fdad(4)	like:6 dislike:3
Msg6	ie821a(5)	like:0 dislike:1
...	.... ....	...

Round  $i+1$

Msg7	829q(-2)	like:1 dislike:1
Msg8	fapqx(1)	like:3 dislike:2
Msg9	zcvbfa(2)	like:1 dislike:2
...	.... ....	...

Round  $i+2$

V.S.

Msg1	csdfsa(100)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	.... ....	...

Round  $i$

Msg4	u78edja(-2)	like:0 dislike:2
Msg5	79fdad(4)	like:6 dislike:3
Msg6	ie821a(101)	like:0 dislike:1
...	.... ....	...

Round  $i+1$

Msg7	829q(-2)	like:1 dislike:1
Msg8	fapqx(100)	like:3 dislike:2
Msg9	zcvbfa(2)	like:1 dislike:2
...	.... ....	...

Round  $i+2$

# Road-Map

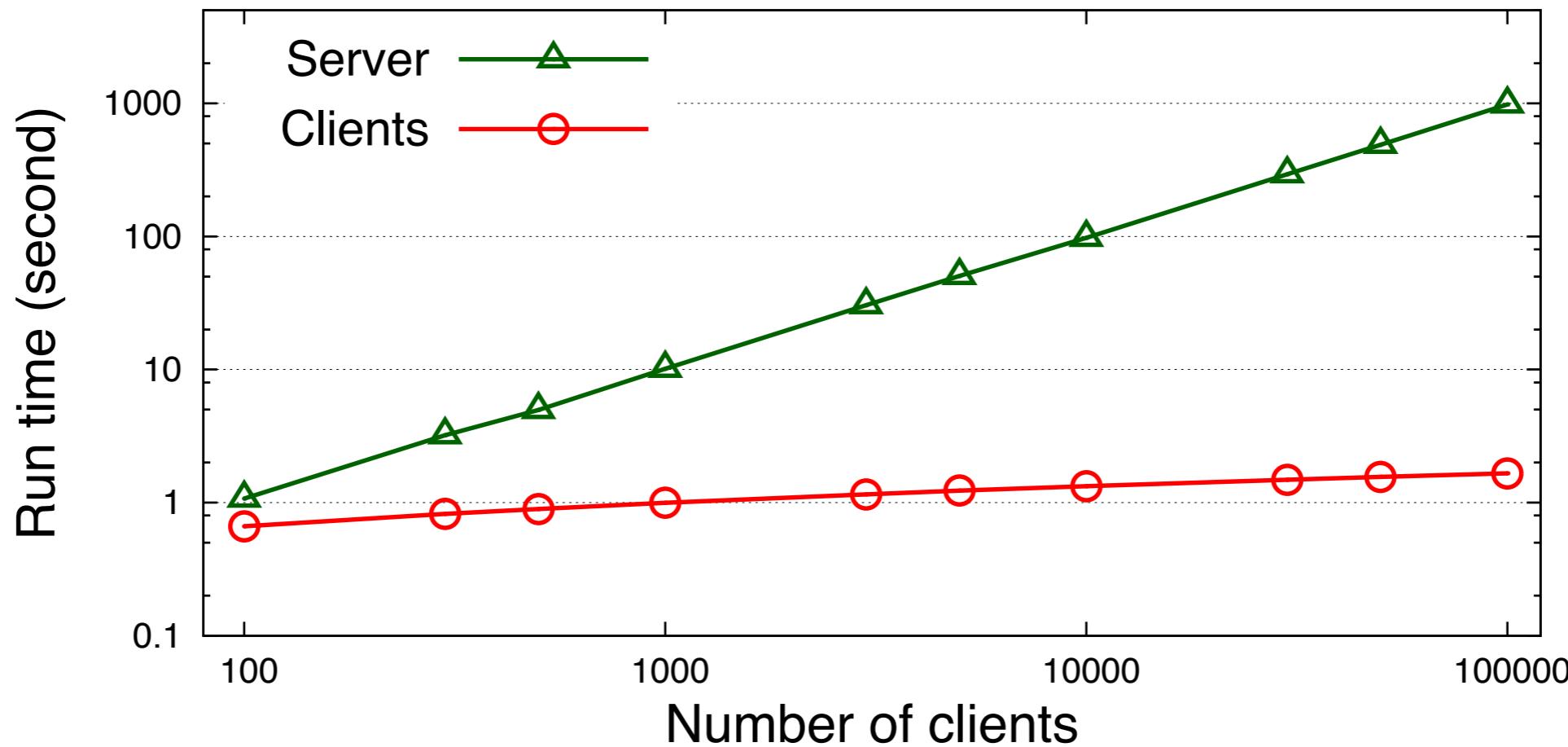
- Motivations
- AnonRep Design
- Practical Considerations
- Evaluation



# Implementation

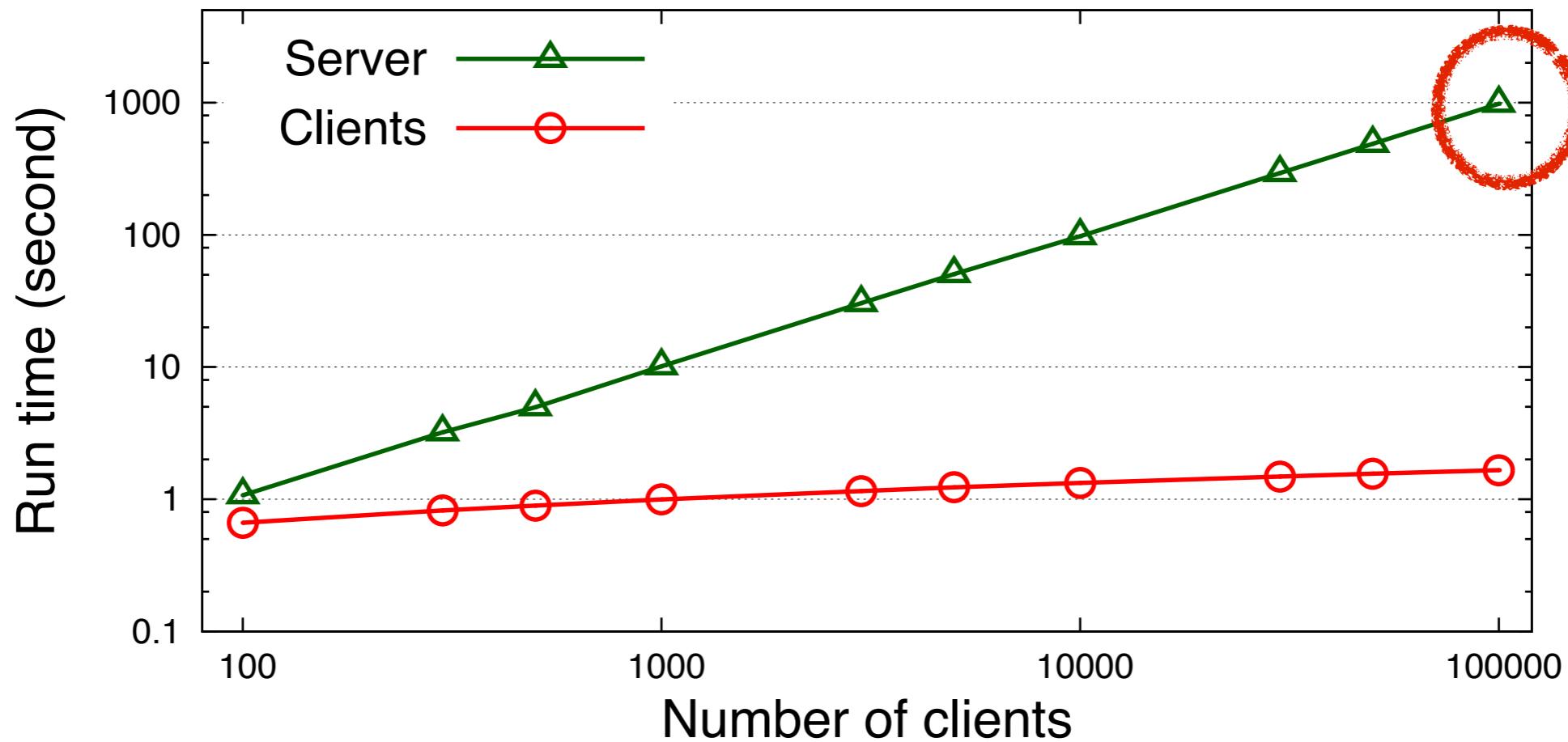
- A working prototype in Go Language
  - Heavily depends on DeDiS Crypto Go library  
<https://github.com/DeDiS/crypto>
  - Our prototype is open source  
<https://github.com/anonyreputation/anonCred>

# Evaluation



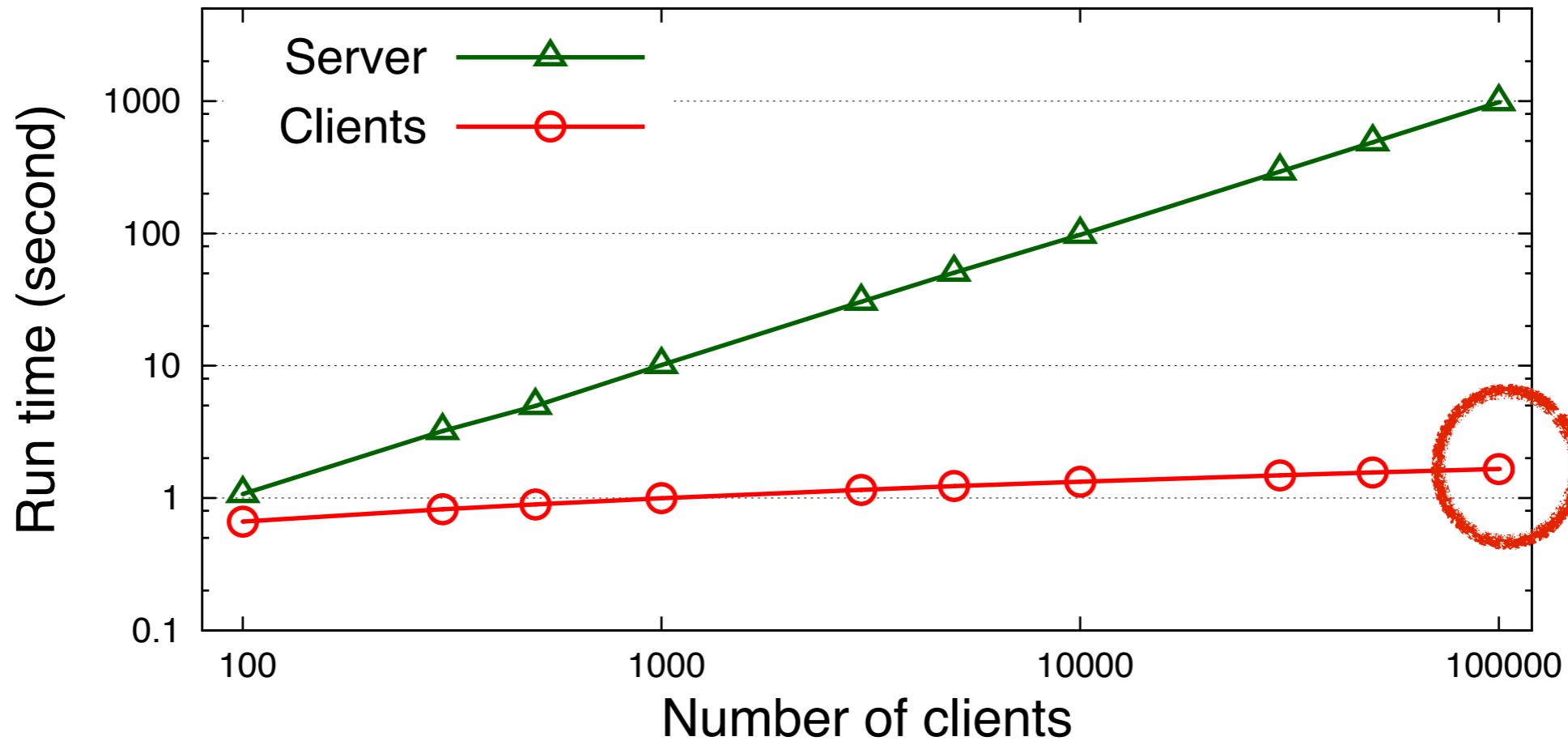
Computational overhead in announcement step

# Evaluation



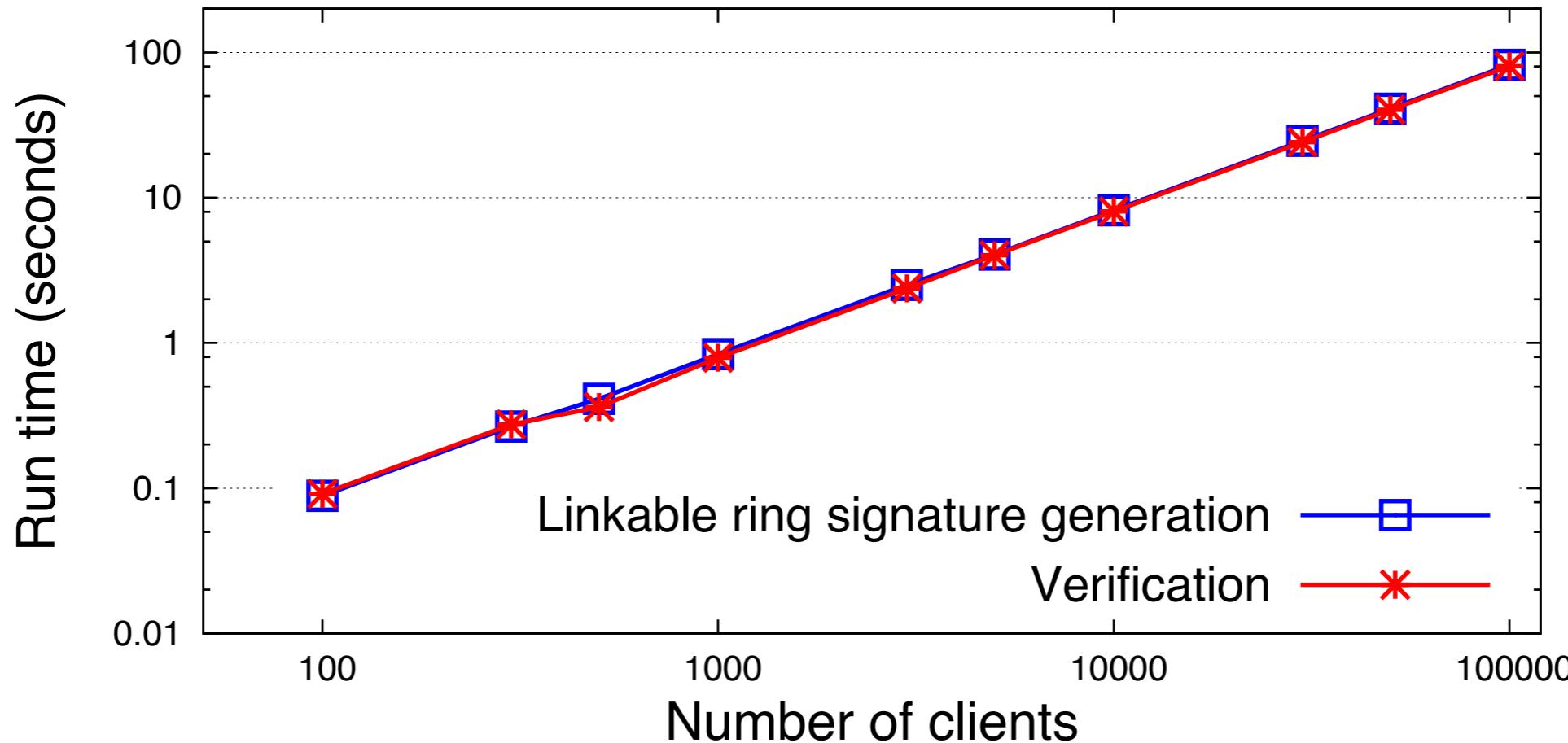
Computational overhead in announcement step

# Evaluation



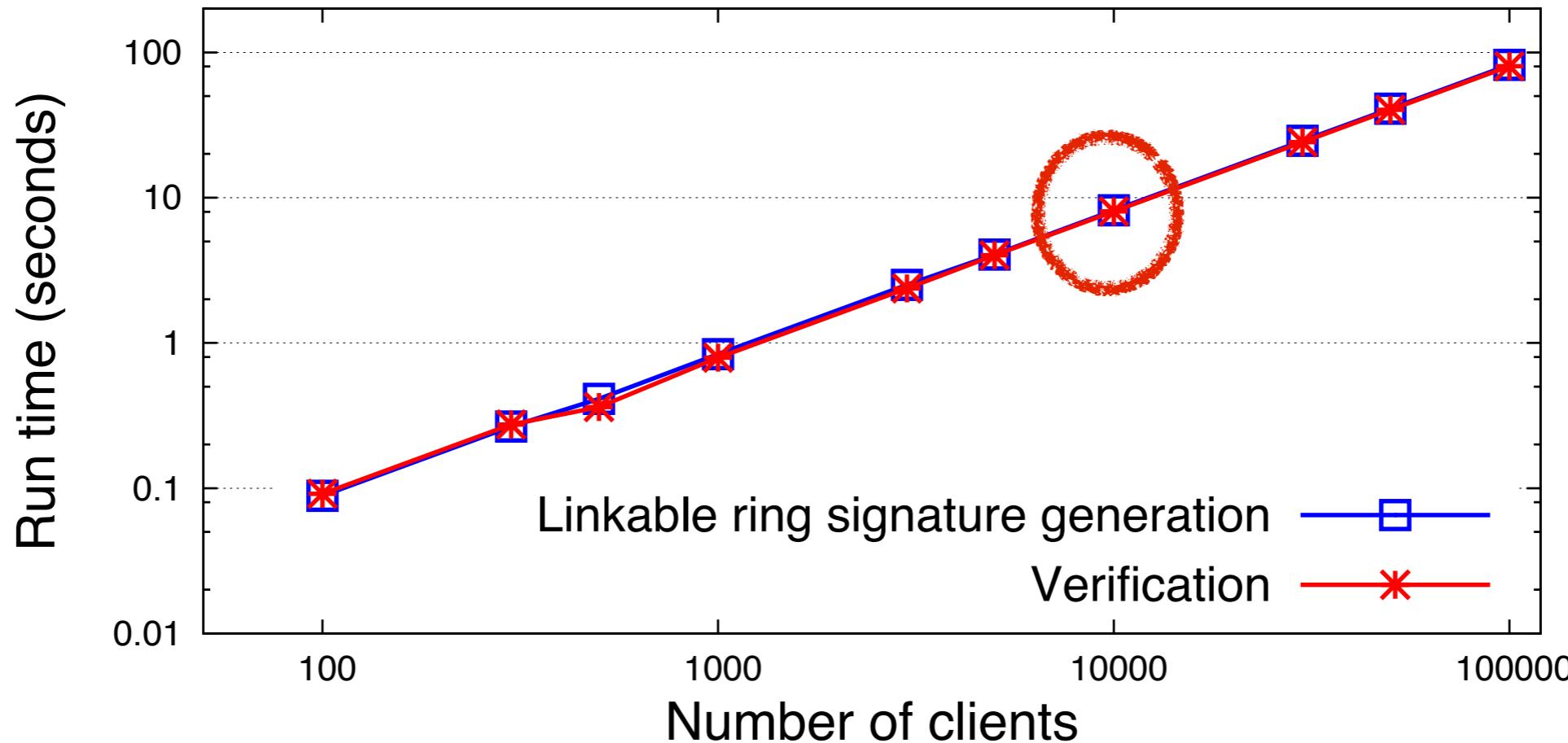
Computational overhead in announcement step

# Evaluation



Computational overhead of feedback step

# Evaluation



Computational overhead of feedback step

# Conclusion

- The first practical tracking-resistant anonymous reputation system:
  - Unlinkability and anonymity of users' activities
  - Diverse reputation utilities (algorithms)
  - No need trust any centralized party
  - Scalable to large-size user set
- Find out more at:
  - <http://dedis.cs.yale.edu/dissent/>