AnonRep: Towards Tracking-Resistant Anonymous Reputation

Ennan Zhai[1]

David Isaac Wolinsky[2], Ruichuan Chen[3],

Ewa Syta[1], Chao Teng[2], Bryan Ford[4]

[1] *Yale* [2] *Facebook* [3] *Bell Labs* [4] *EPFL*

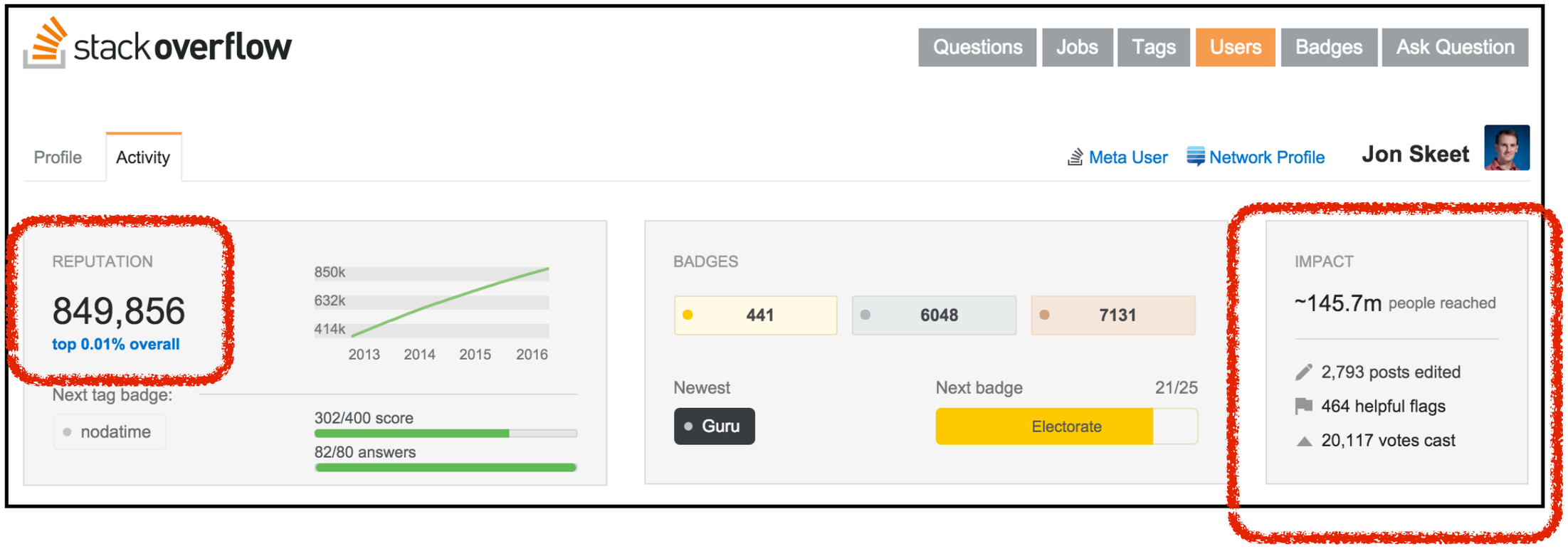
Background

- There is too much information on today's Internet

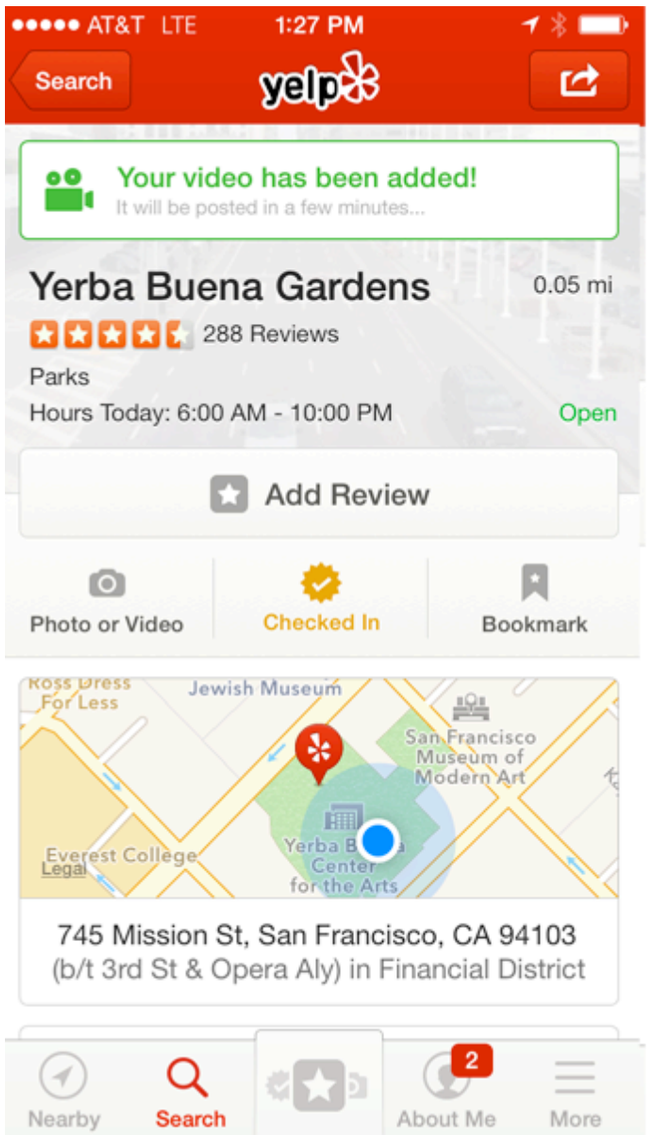
Background

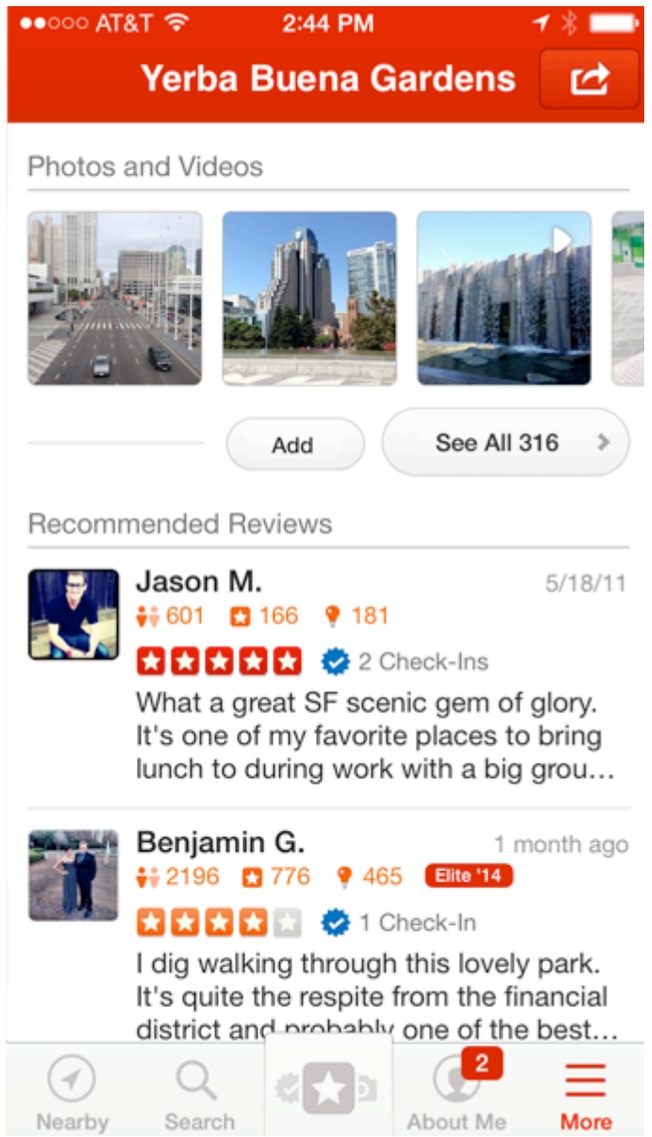
- There is too much information on today's Internet
- Reputation systems are employed:
  - Highlighting information quality
  - Filtering spam

Stack Overflow

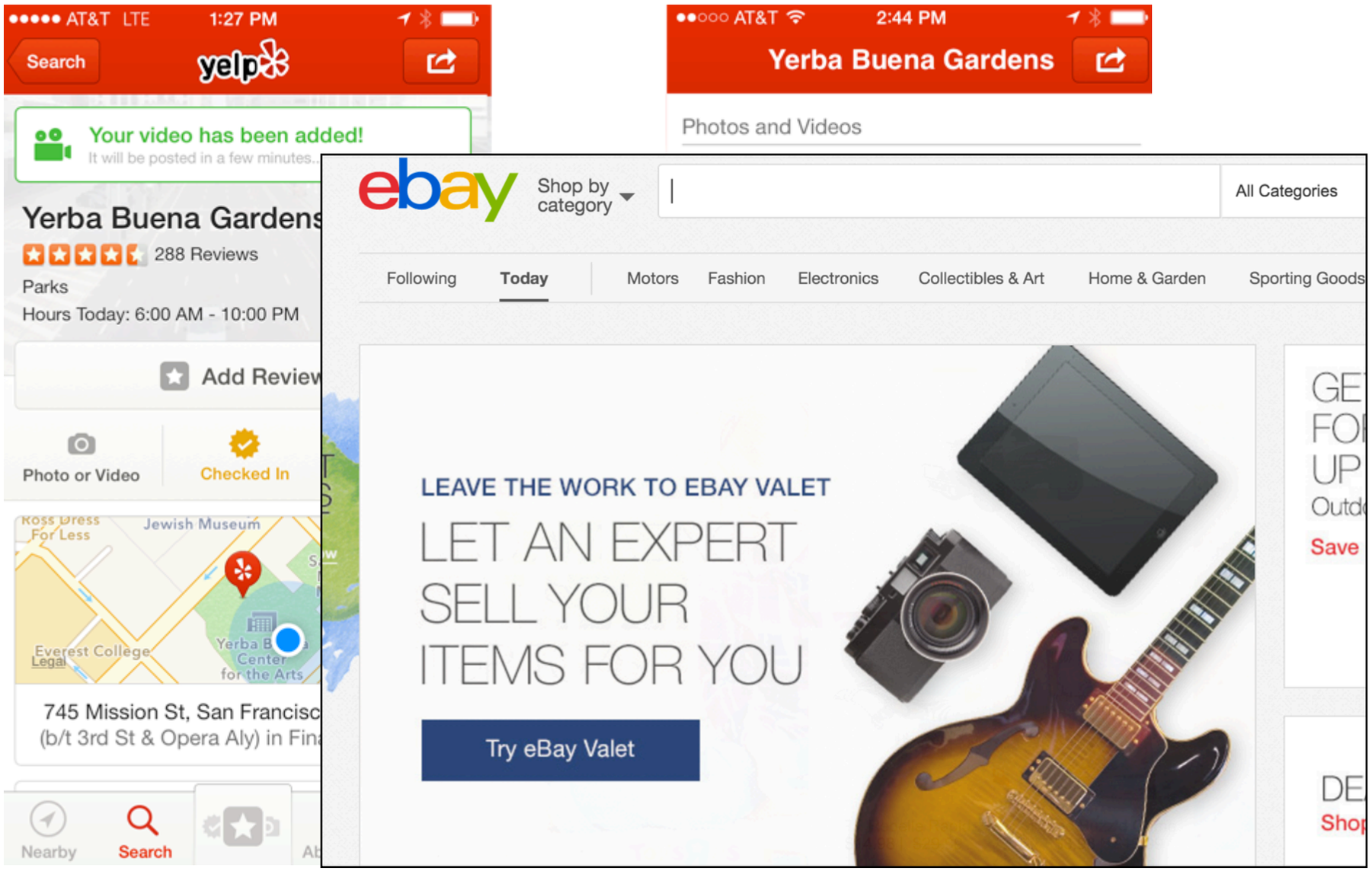


Reputation System

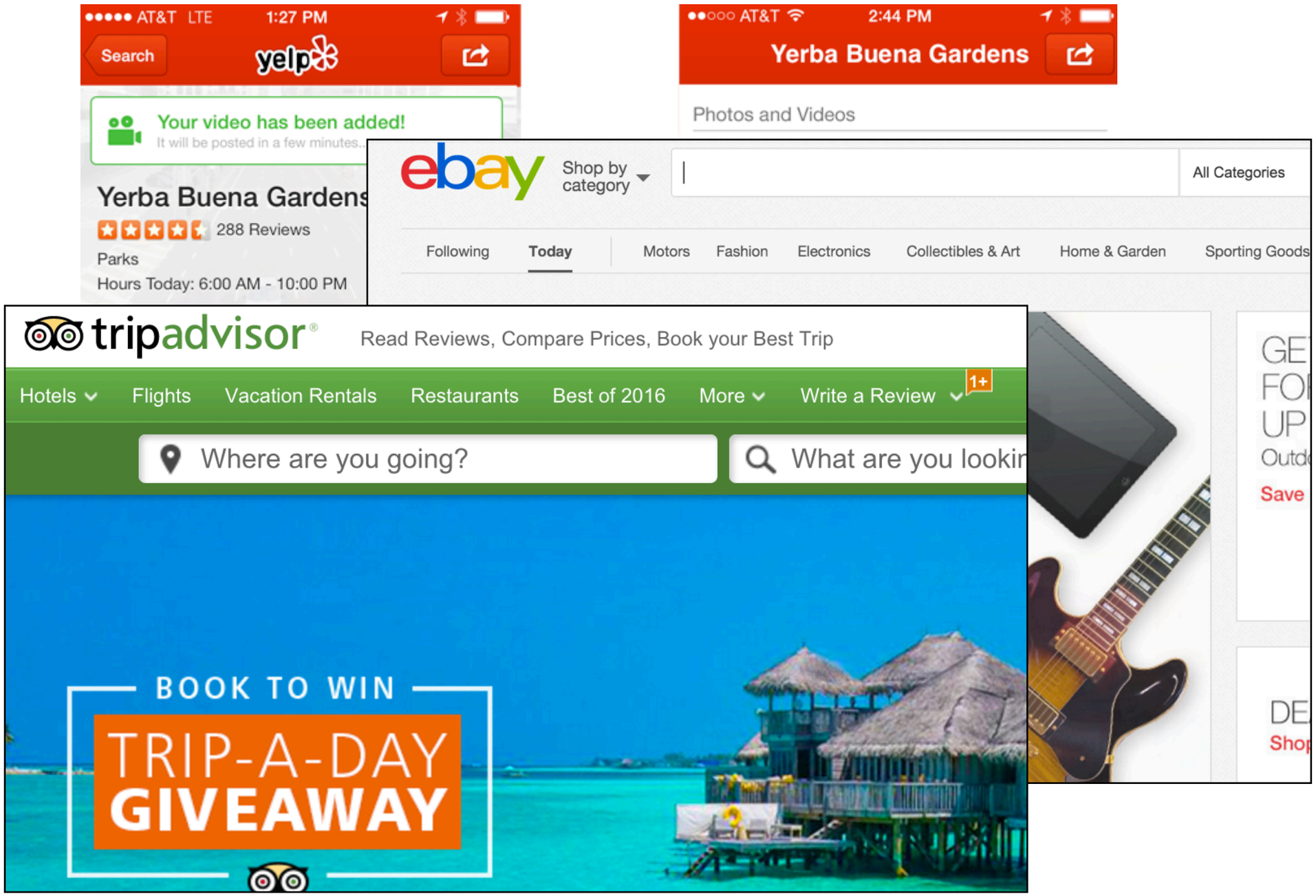




Reputation System



Reputation System



Reputation System

Messages	Author (Score)	Votes
…	…	
…	…	
…	…	
…	…	

Reputation System

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

Reputation System

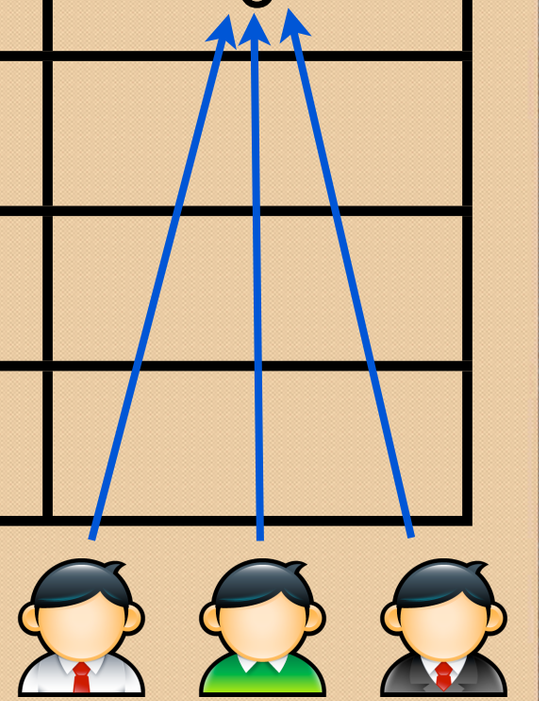
Messages	Author (Score)	Votes
I like NSDI'16	Alice (0)	0
…	…	
…	…	
…	…	

Reputation System

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

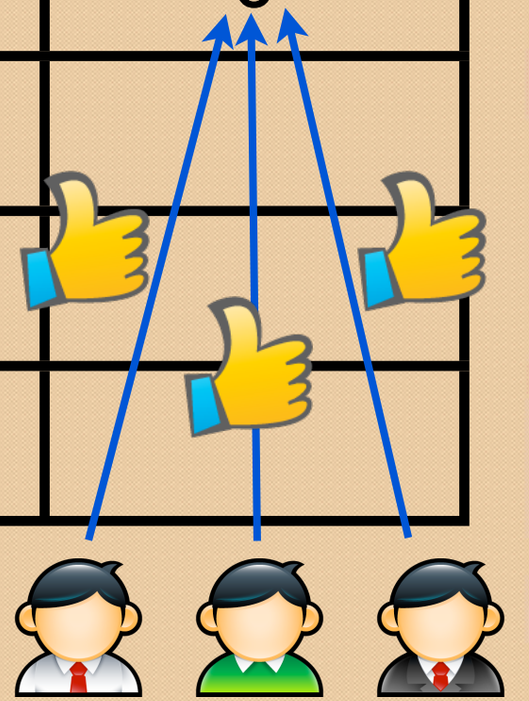
Reputation System

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



Reputation System

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



Bob Eve Dave

Reputation System

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

Reputation System

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

$\sum V_i = 1+1+1 = 3$

Reputation System

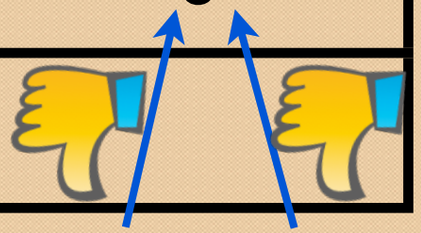
Messages	Author (Score)	Votes
I like NSDI'16	Alice (3)	Like: 3
Don't play with AlphaGo	Alice (3)	0
...	...	
...	...	

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
...	...	

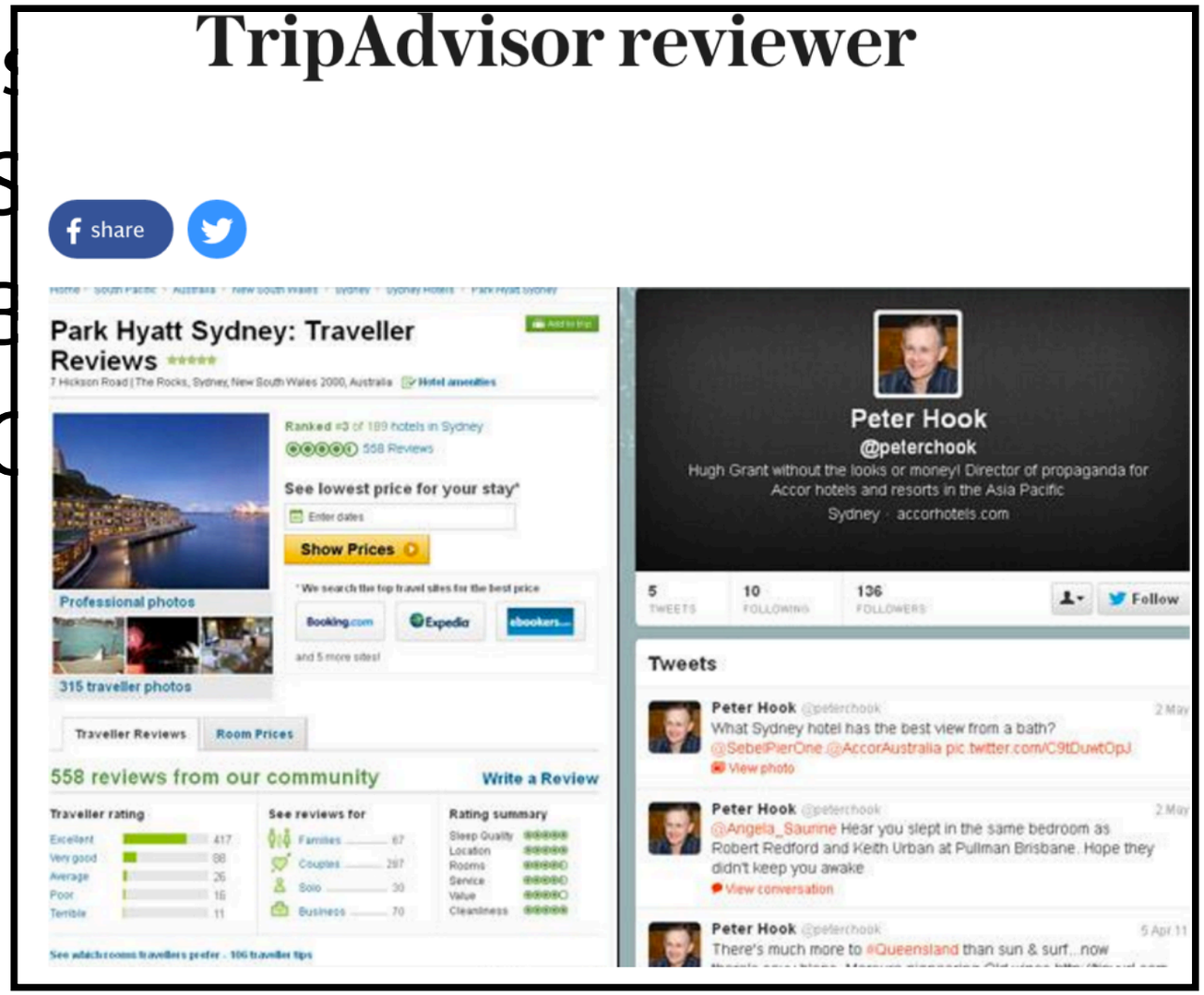
$\sum V_i = 1-1-1 = -1$

People Care About Privacy

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

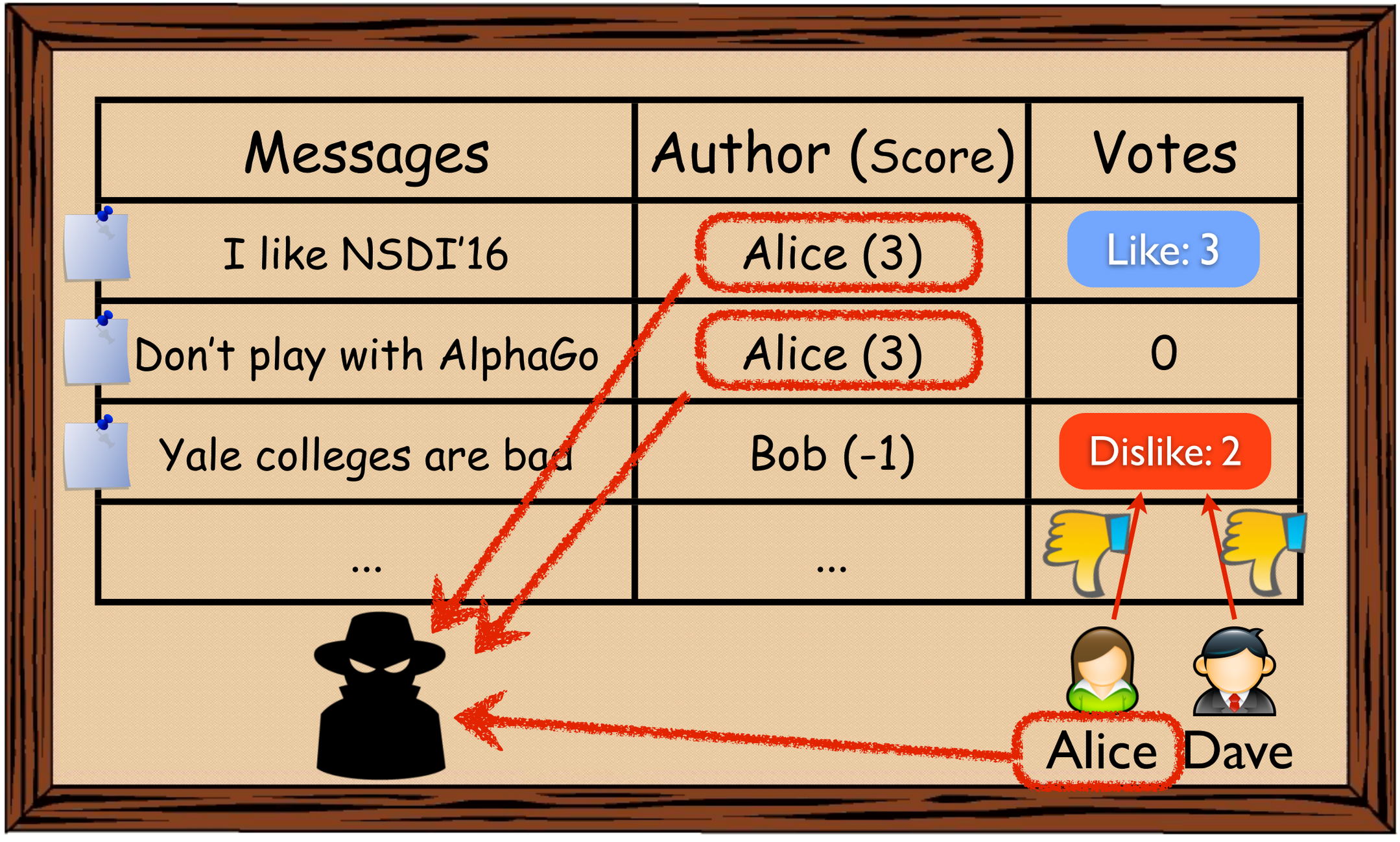
People Care About Privacy

- People want to participate in these reputation sy
  - S
  - B
  - C

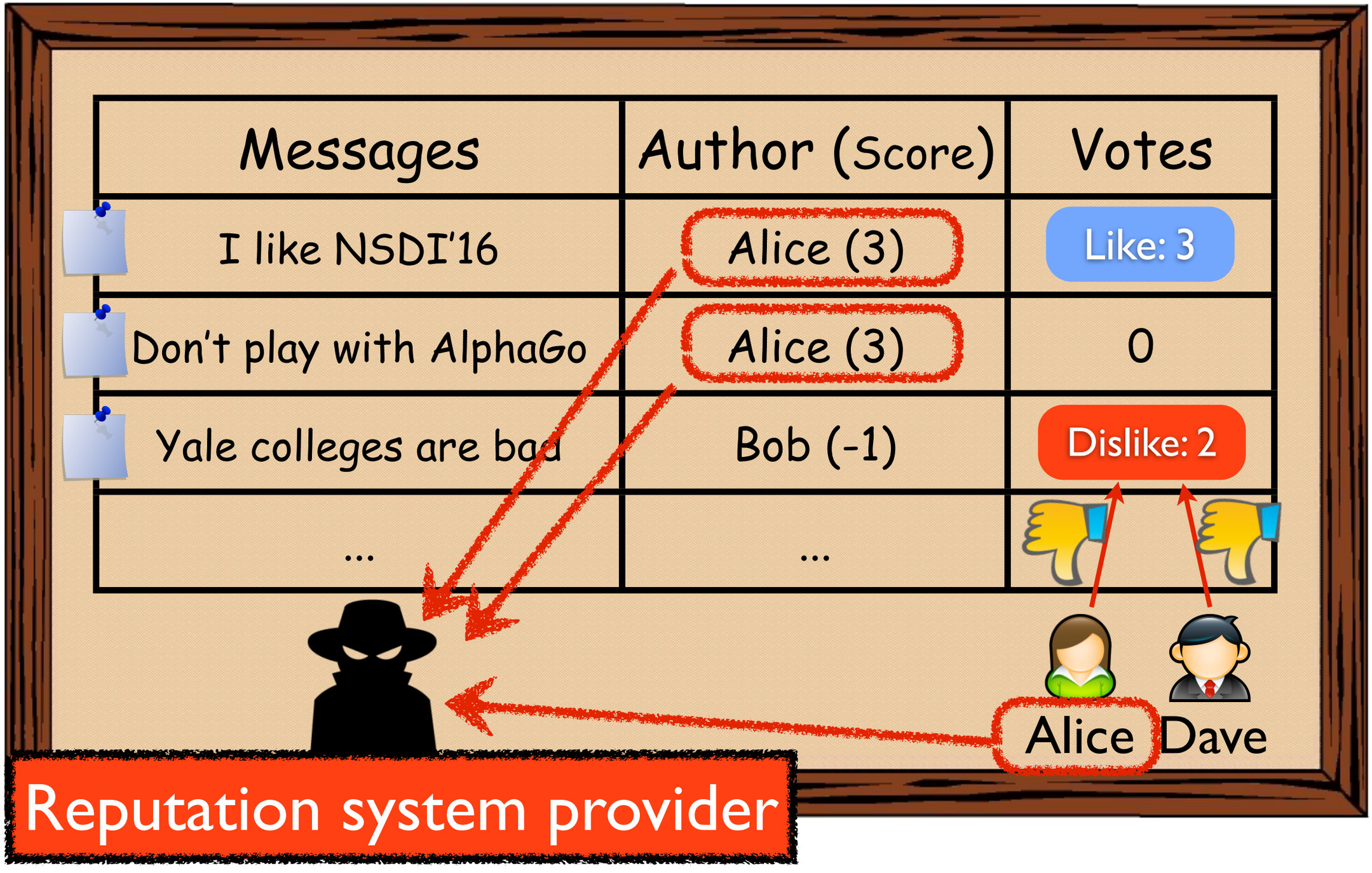


TARGET: Linkability Problem

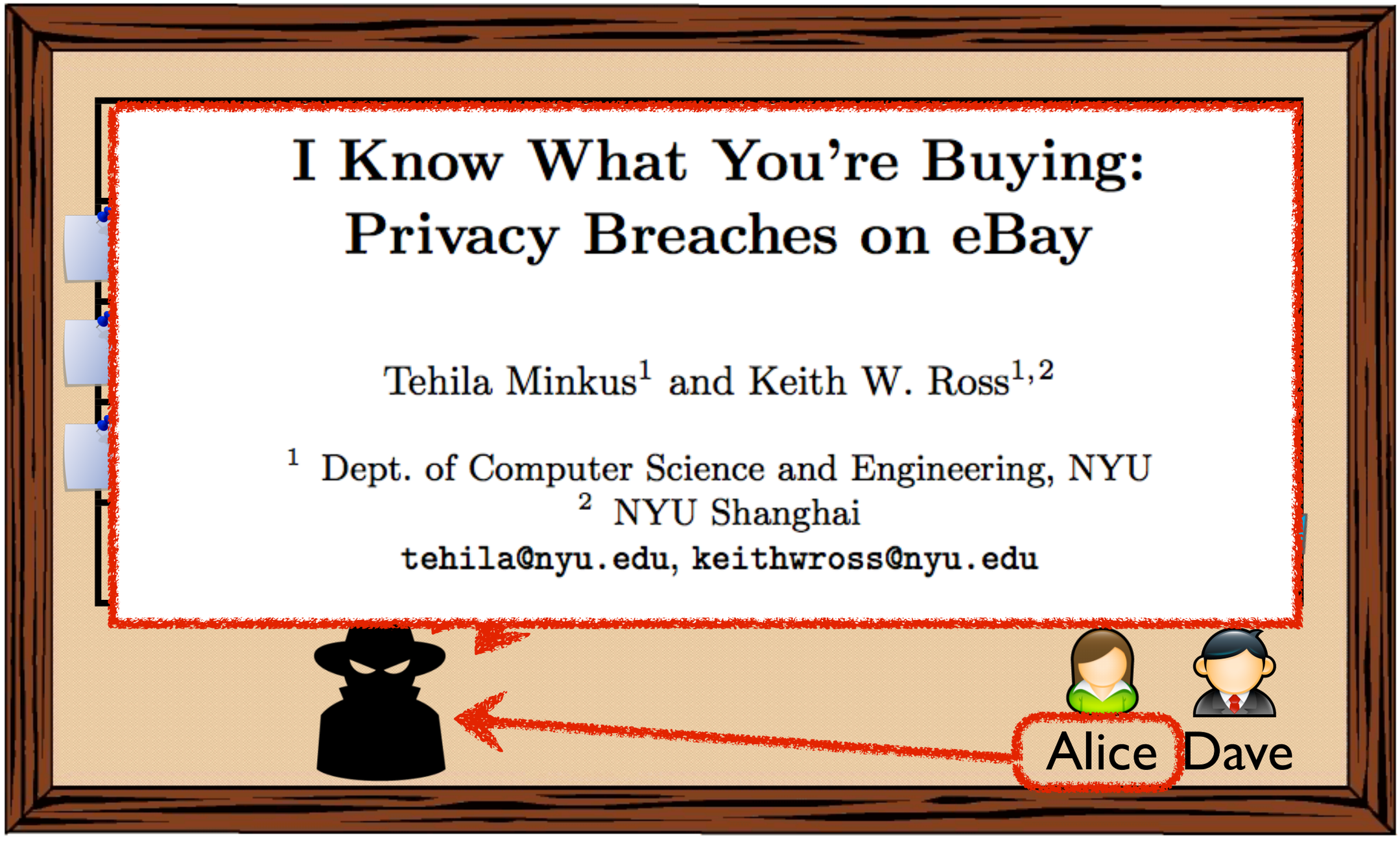
TARGET: Linkability Problem



TARGET: Linkability Problem



TARGET: Linkability Problem



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.

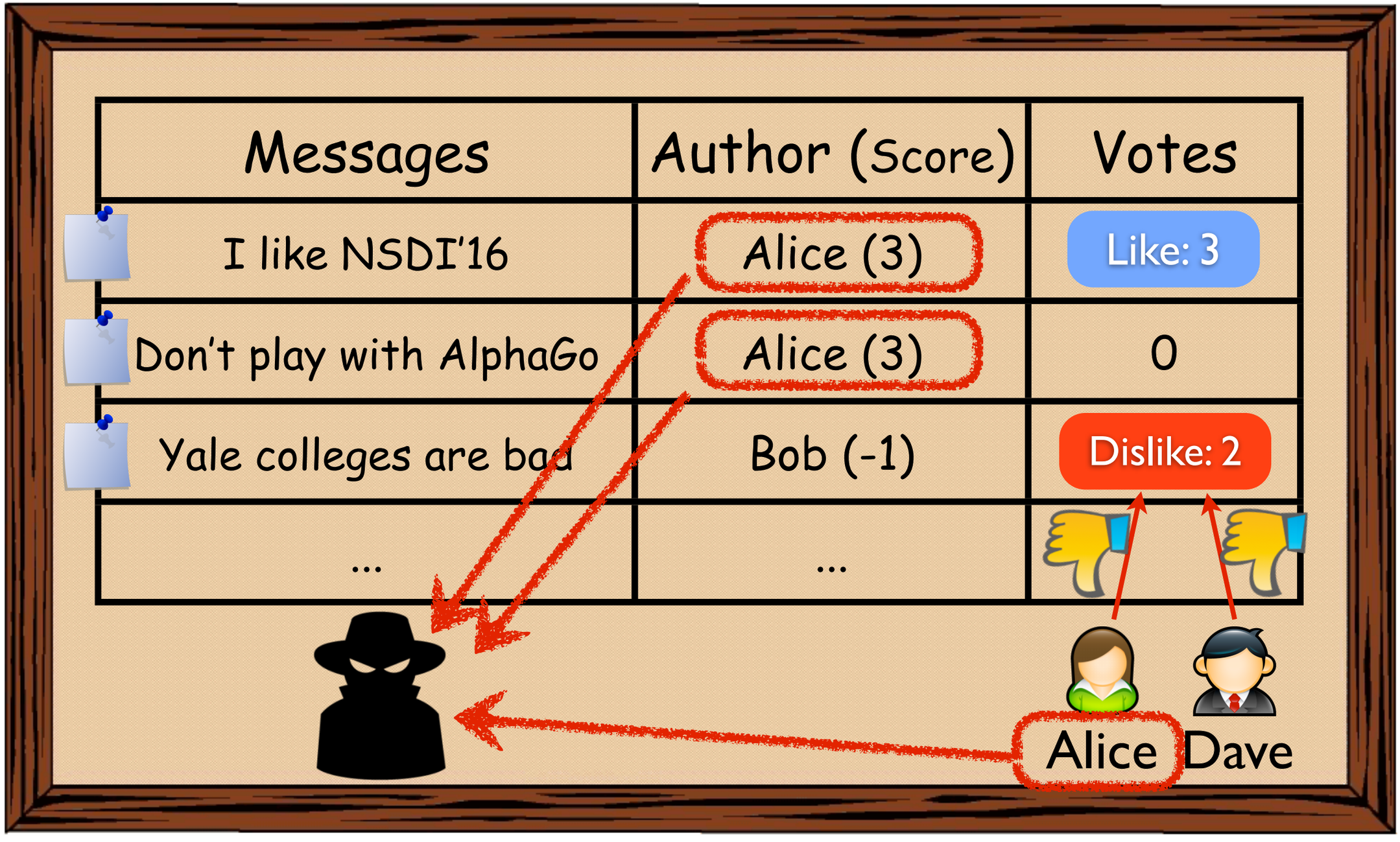
Our Goals

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

Our Goals

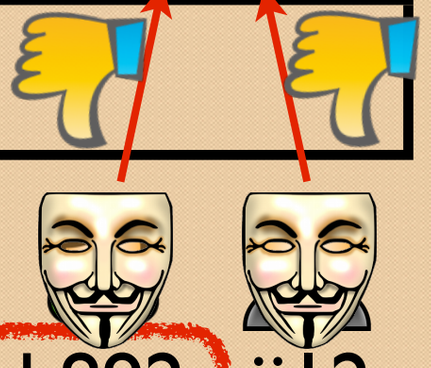
- Tracking-resistant anonymous reputation:
  - Unlinkability and anonymity of users' activities
  - Diverse reputation utilities (algorithms)
  - No need trust any centralized party
  - Scalable to large-size user set

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 b…	3fio (-1)	Dislike: 2
…	…	



k892 jil2

Technical Challenges

Technical Challenges

- Reputation update relies on activities tracking

It is a paradox in practice!

Technical Challenges

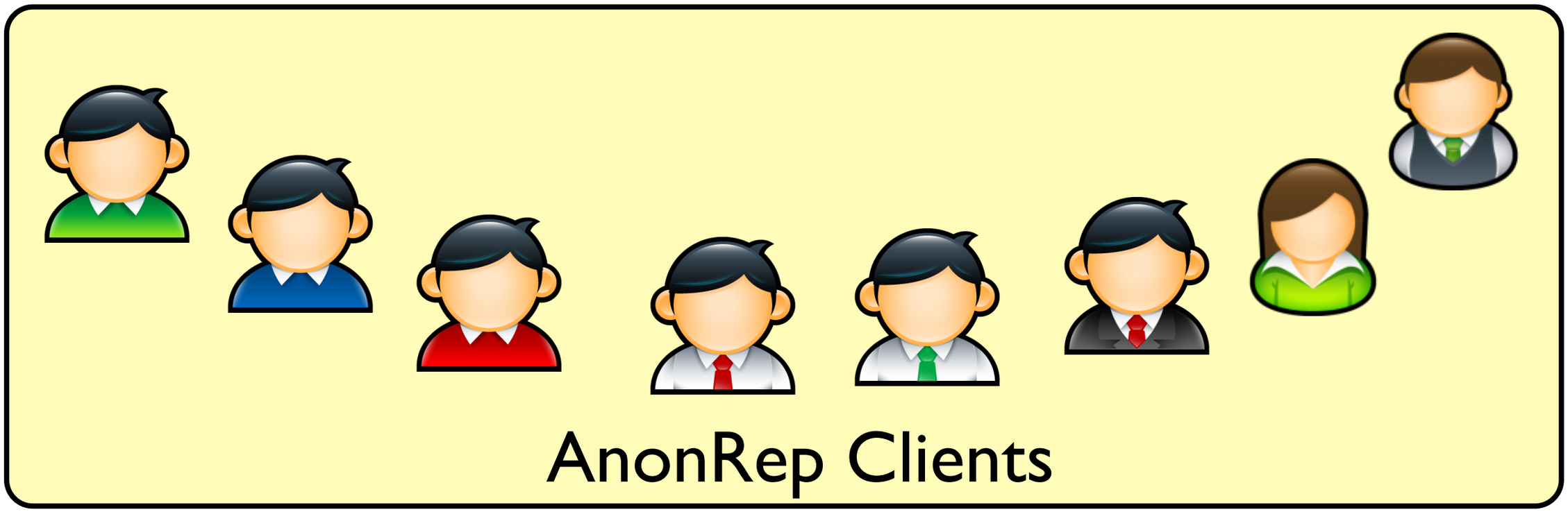
- Reputation update relies on activities tracking
- Misbehaviors (e.g., duplicate voting) detection

Road-Map

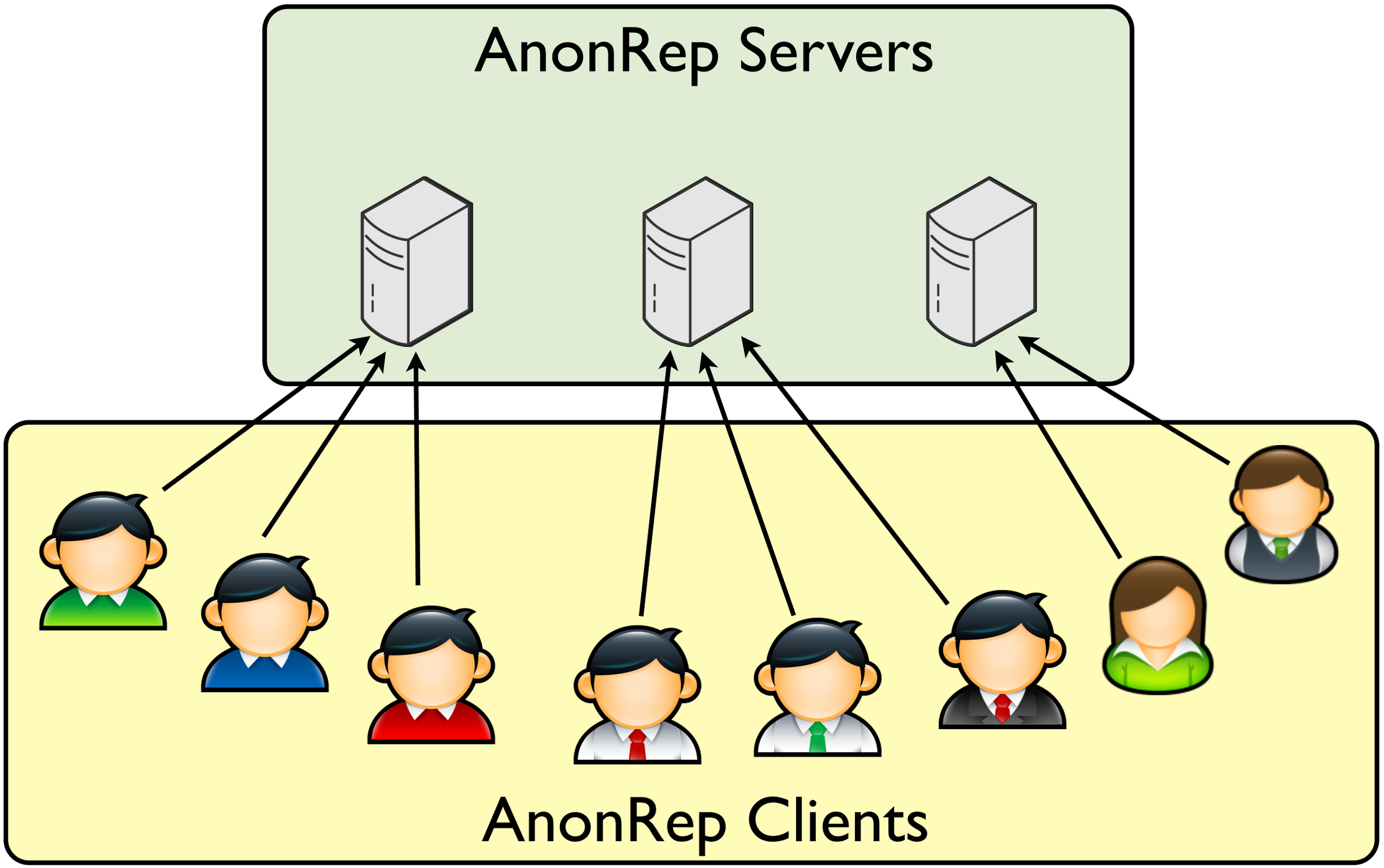
- Motivations
- AnonRep Design
- Practical Considerations
- Evaluation

AnonRep Deployment

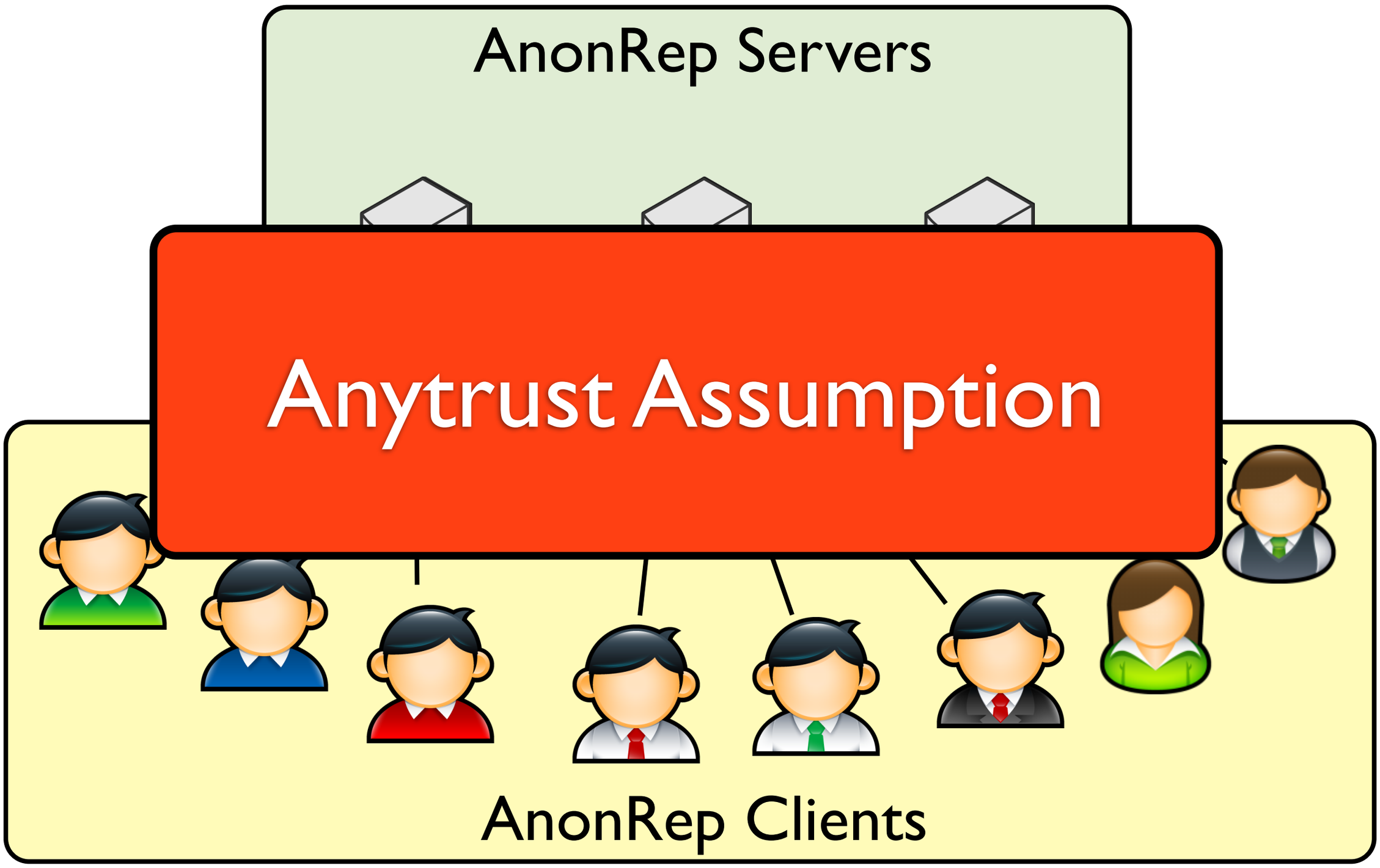
AnonRep Deployment



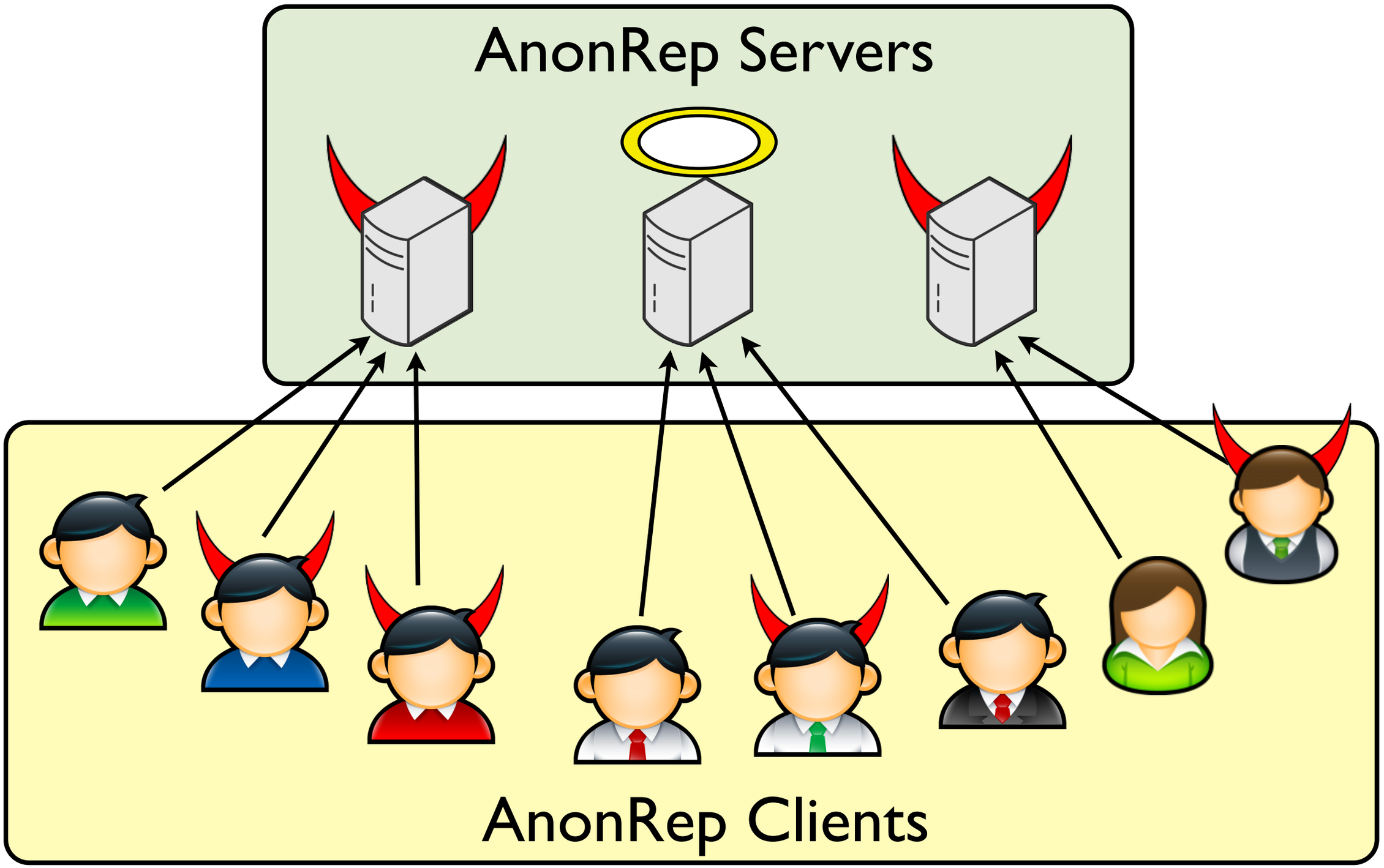
AnonRep Deployment



Threat Model

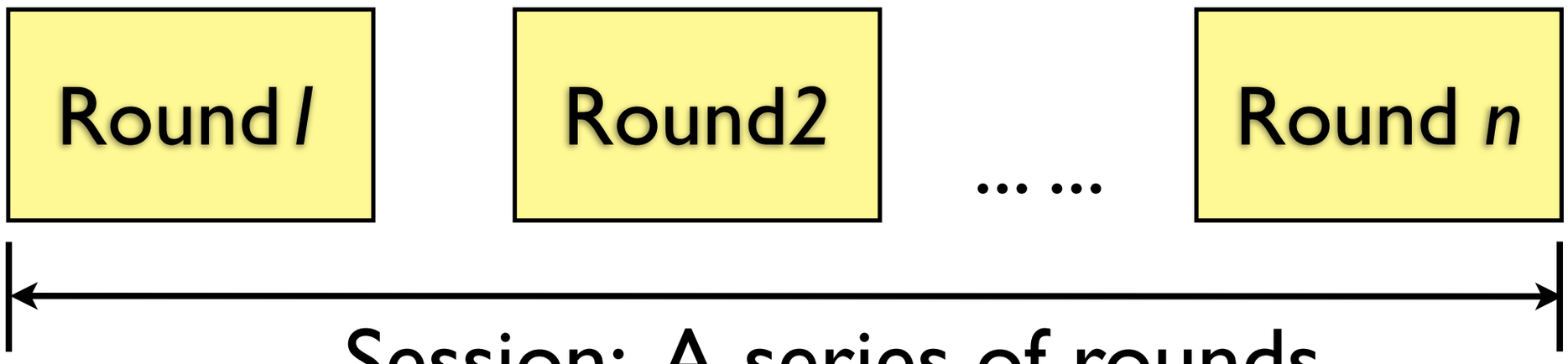


Threat Model



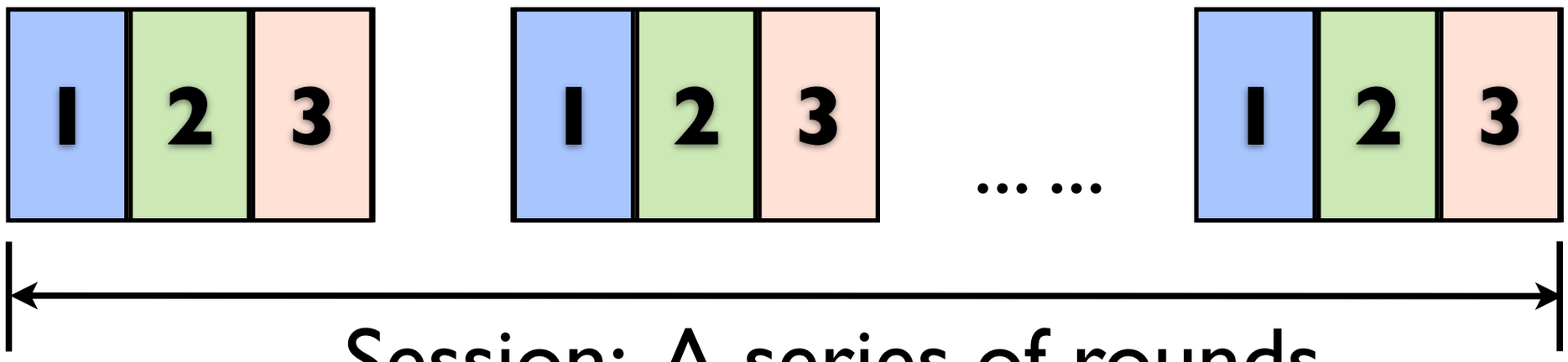
AnonRep Workflow

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



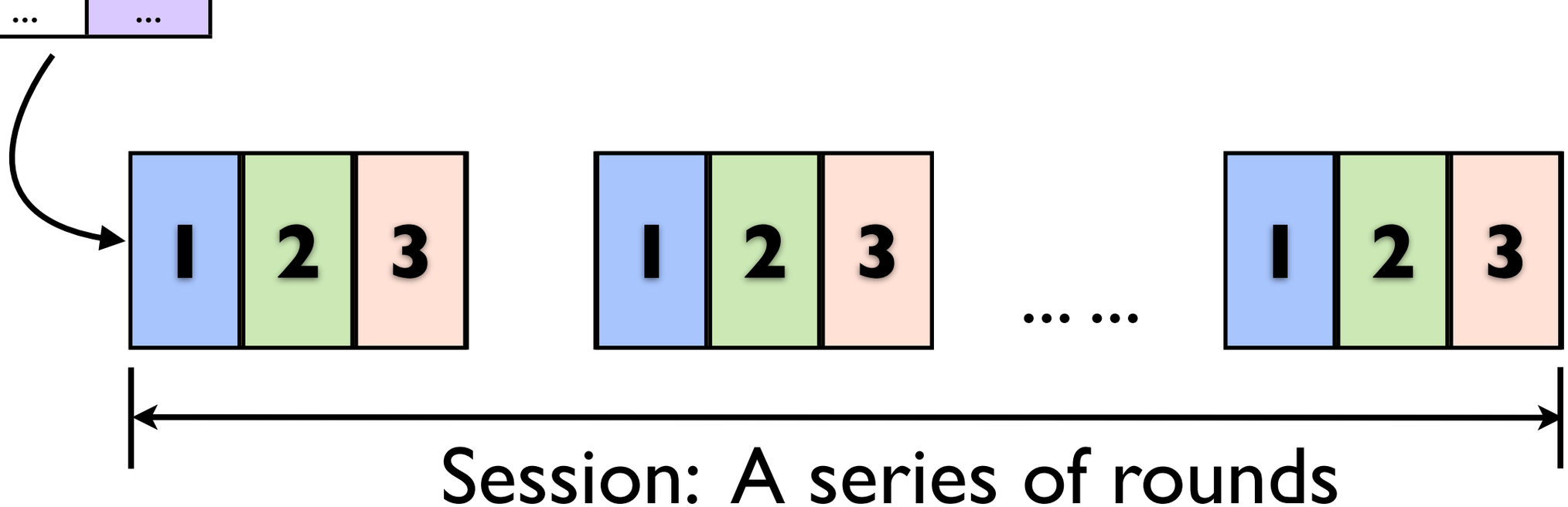
AnonRep Workflow

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

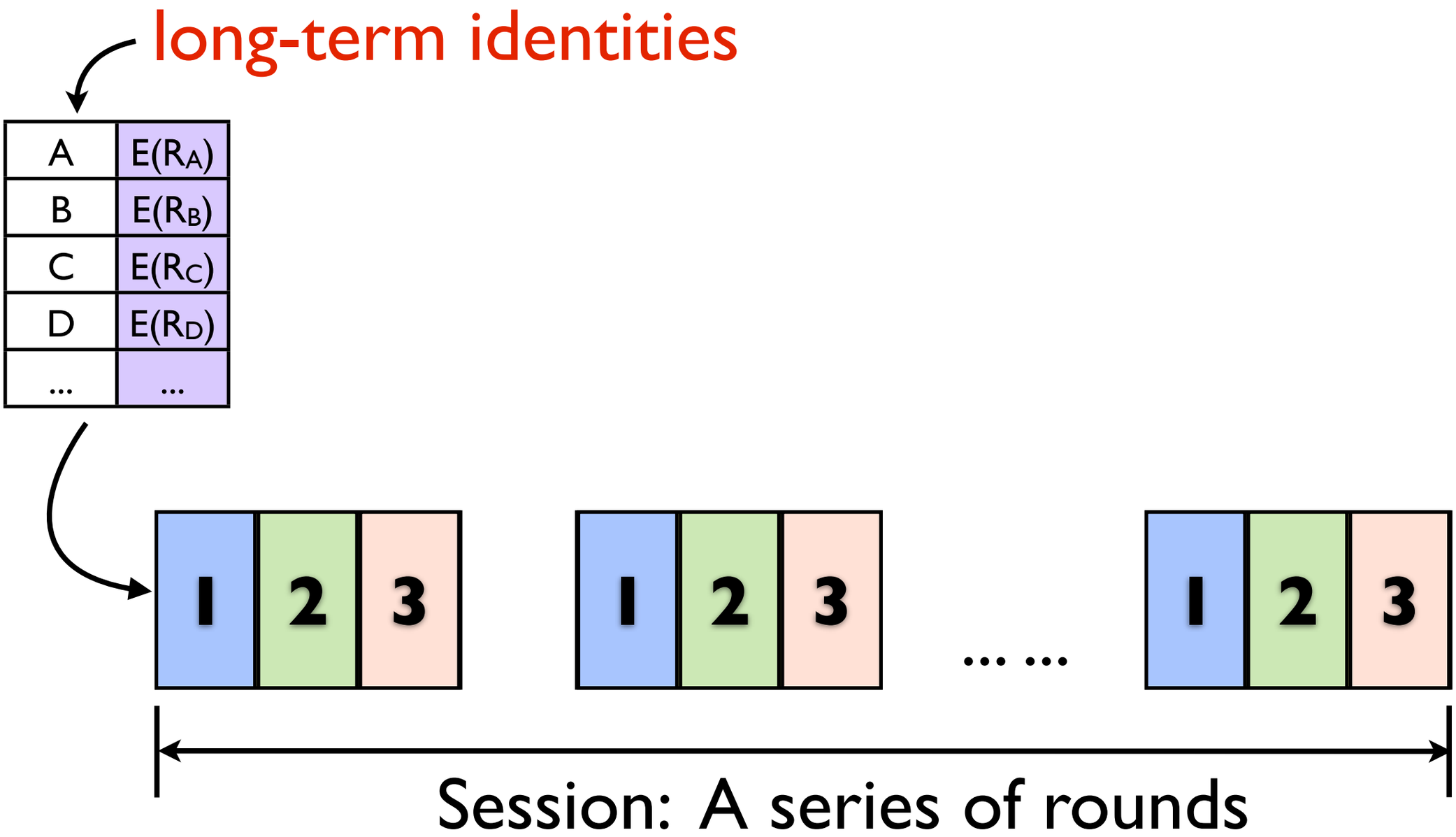


AnonRep Workflow

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



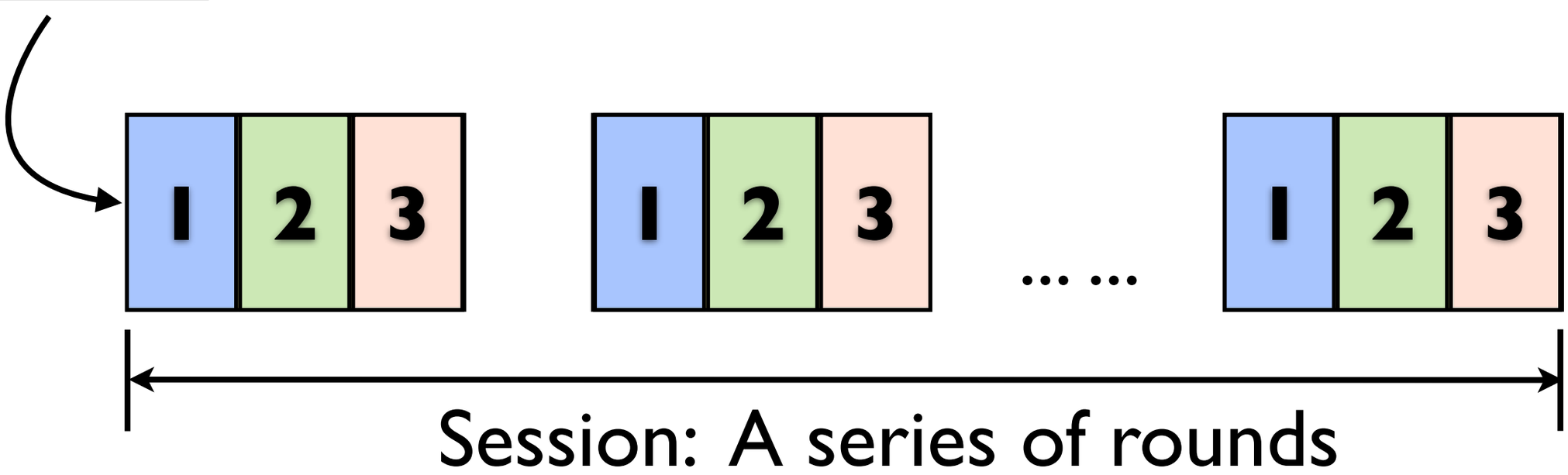
AnonRep Workflow



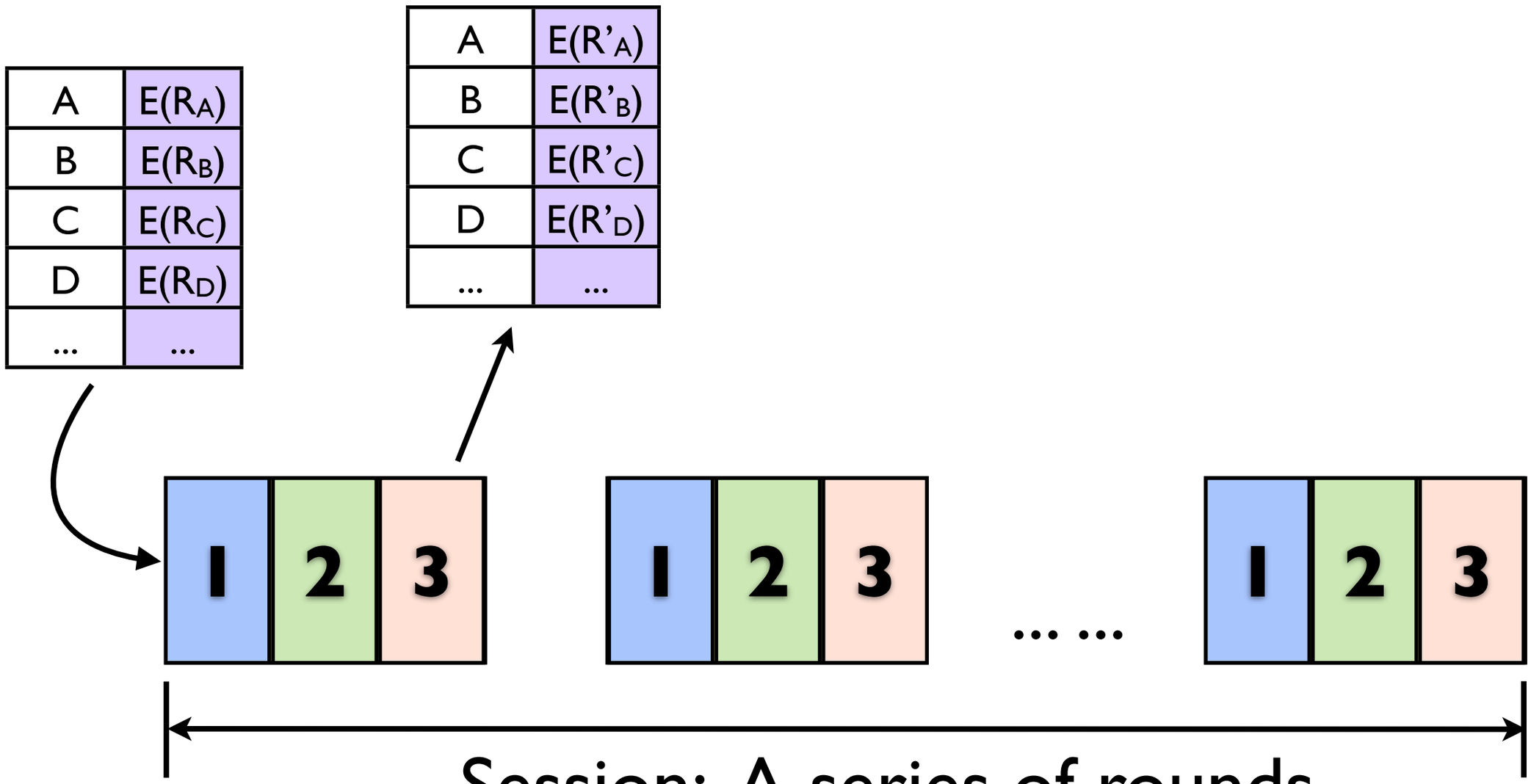
AnonRep Workflow

Reputation ciphertexts,
encrypted by all the servers

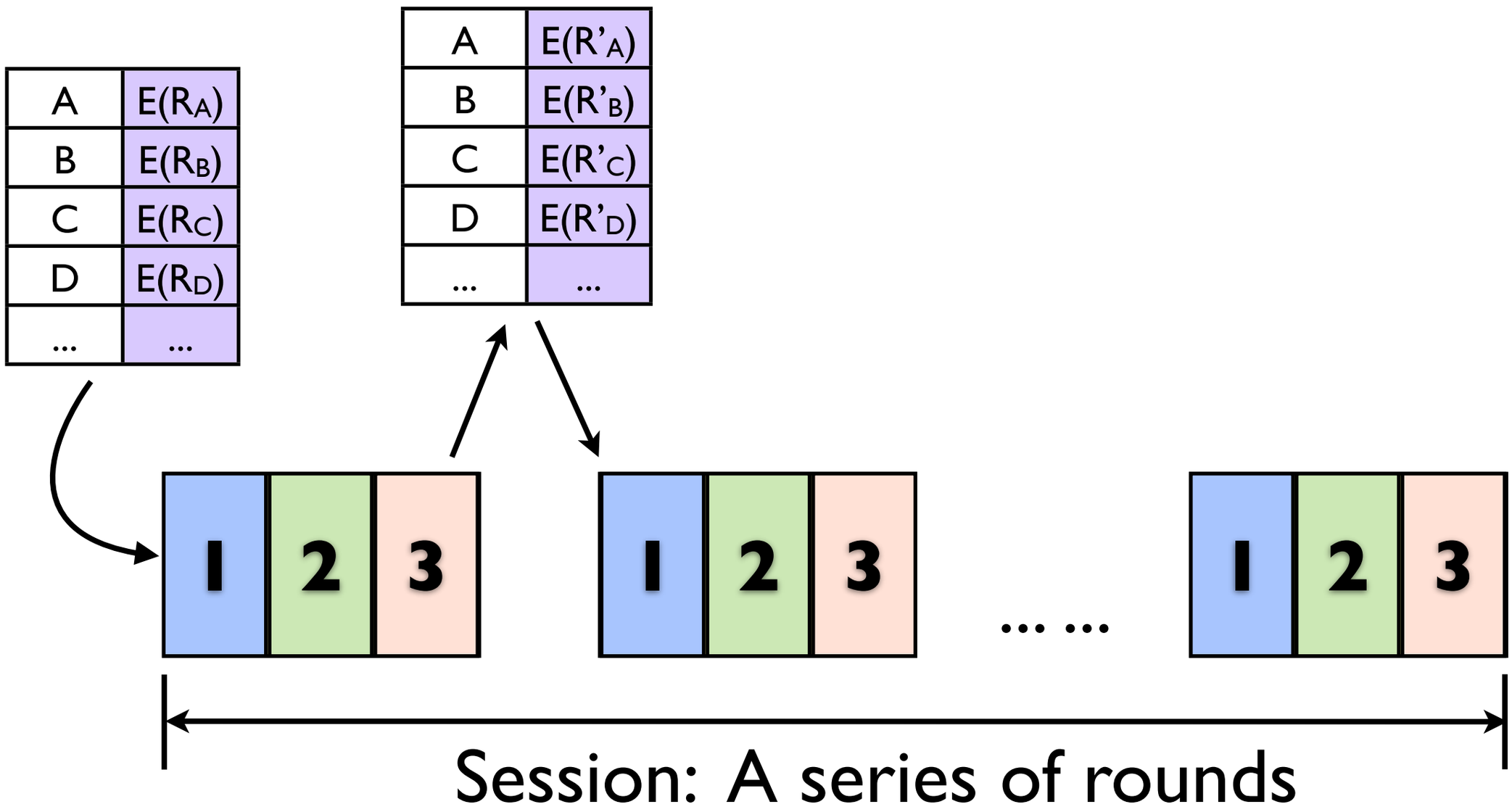
A	$E(R_A)$
B	$E(R_B)$
C	$E(R_C)$
D	$E(R_D)$
...	...



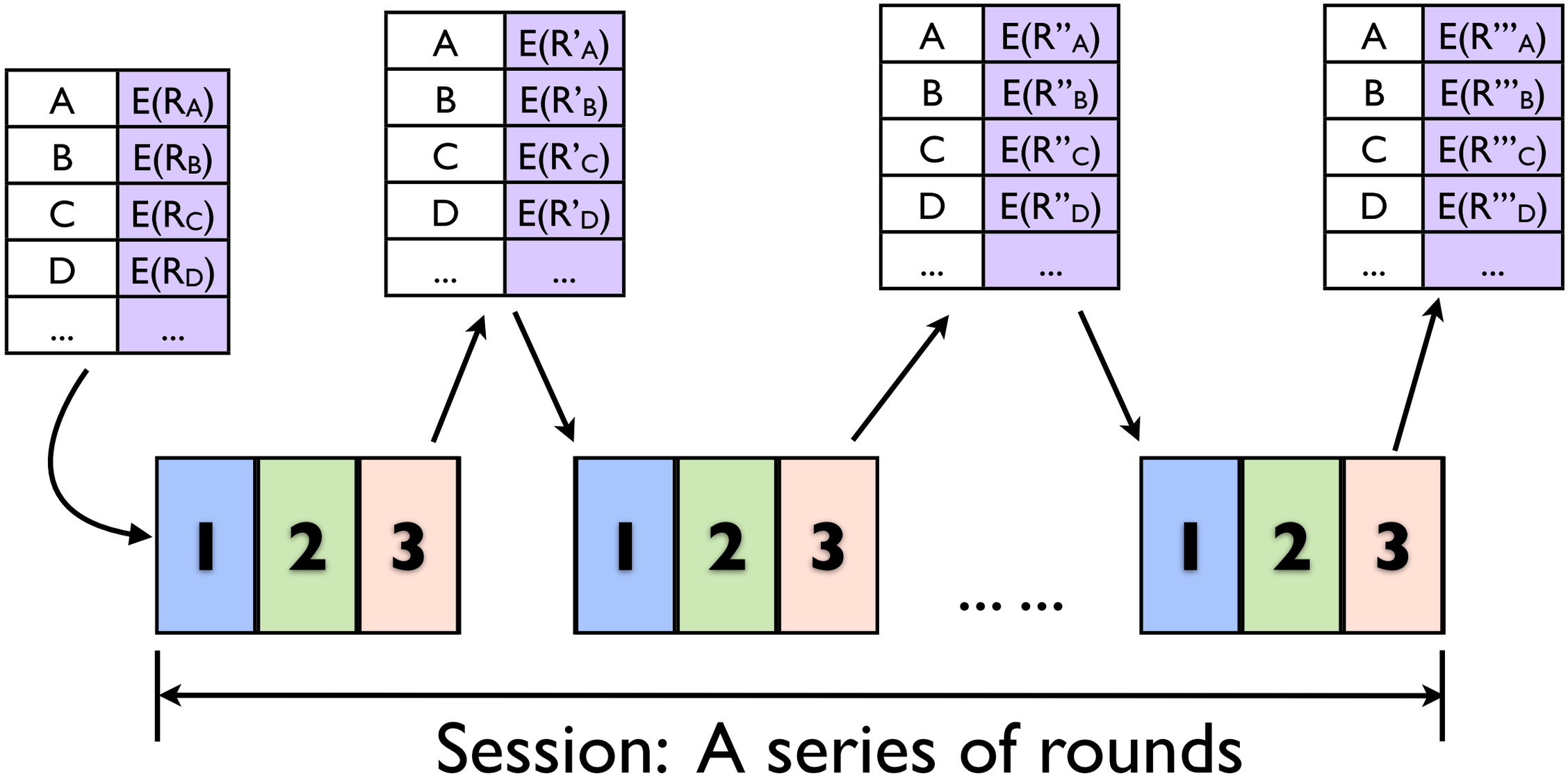
AnonRep Workflow



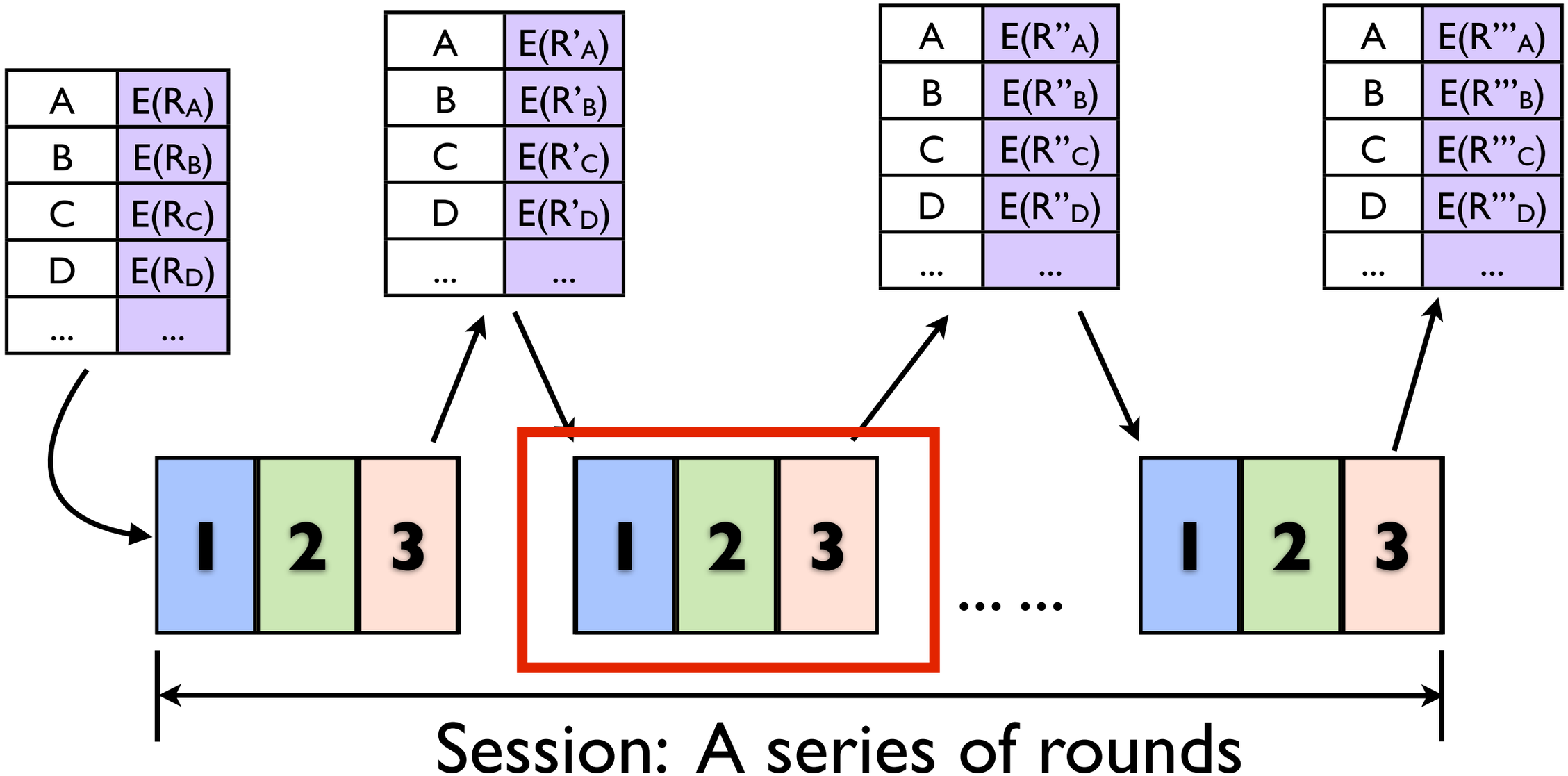
AnonRep Workflow



AnonRep Workflow



AnonRep Workflow

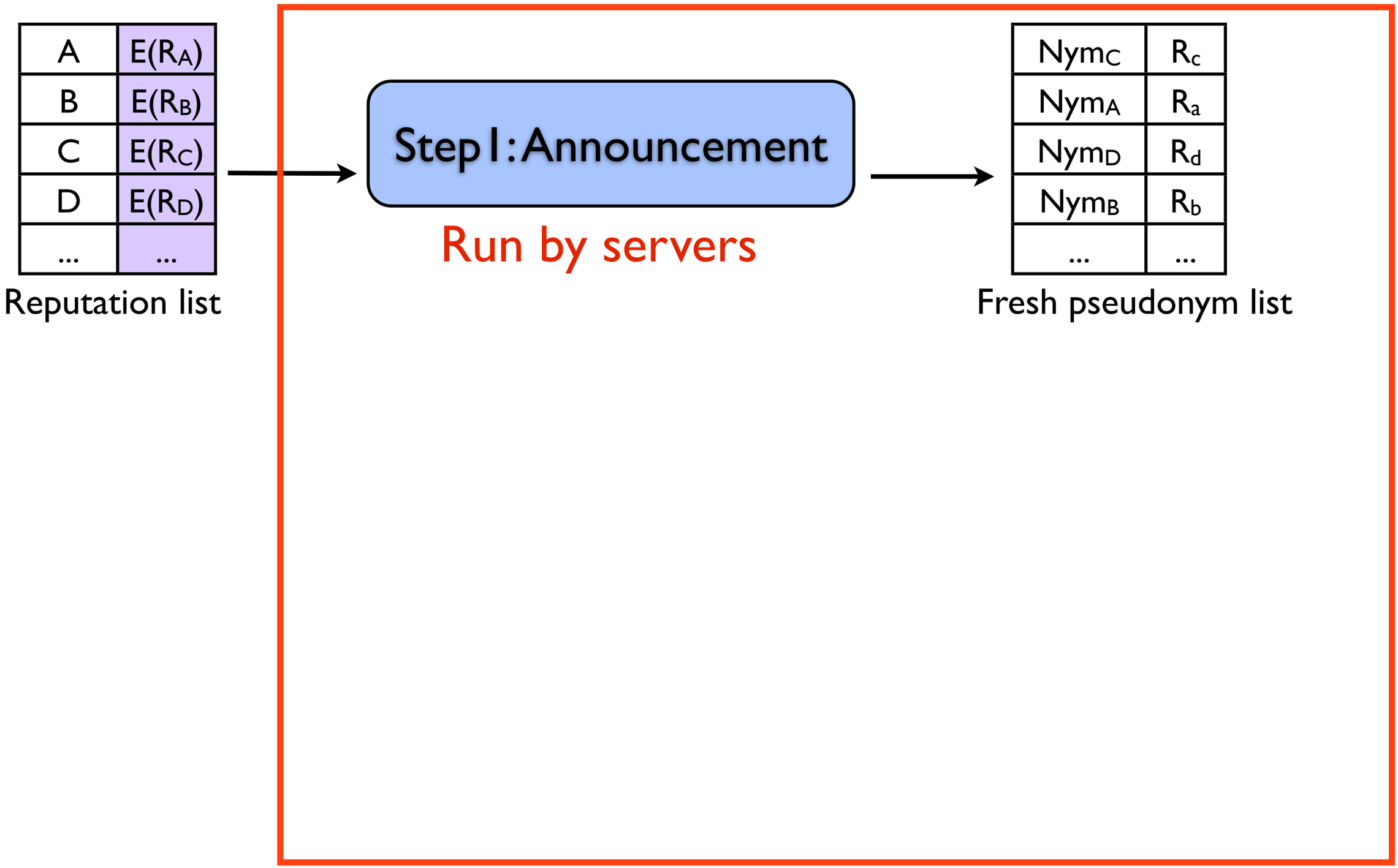


Three Steps in Each Round

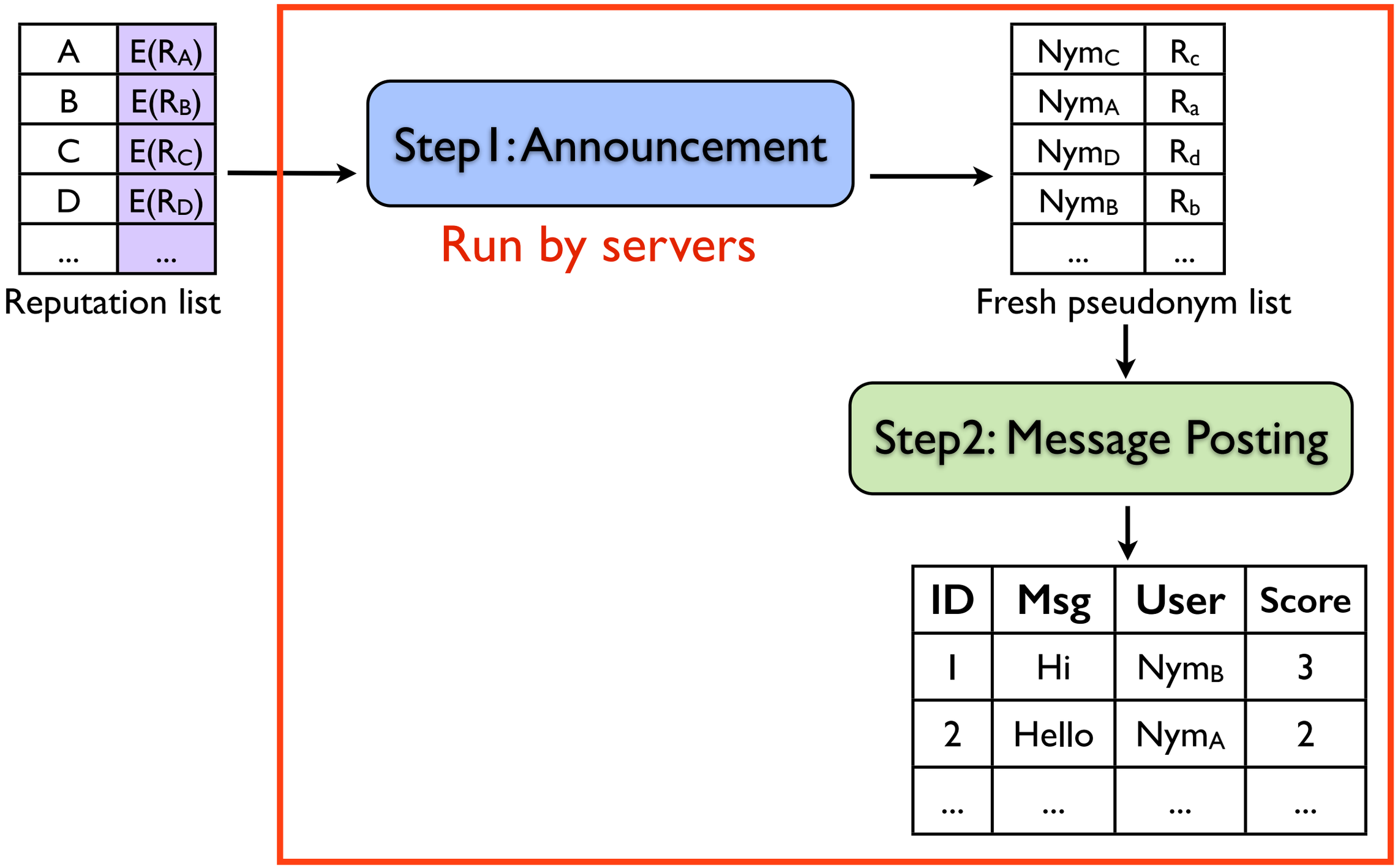
A	$E(R_A)$
B	$E(R_B)$
C	$E(R_C)$
D	$E(R_D)$
...	...

Reputation list

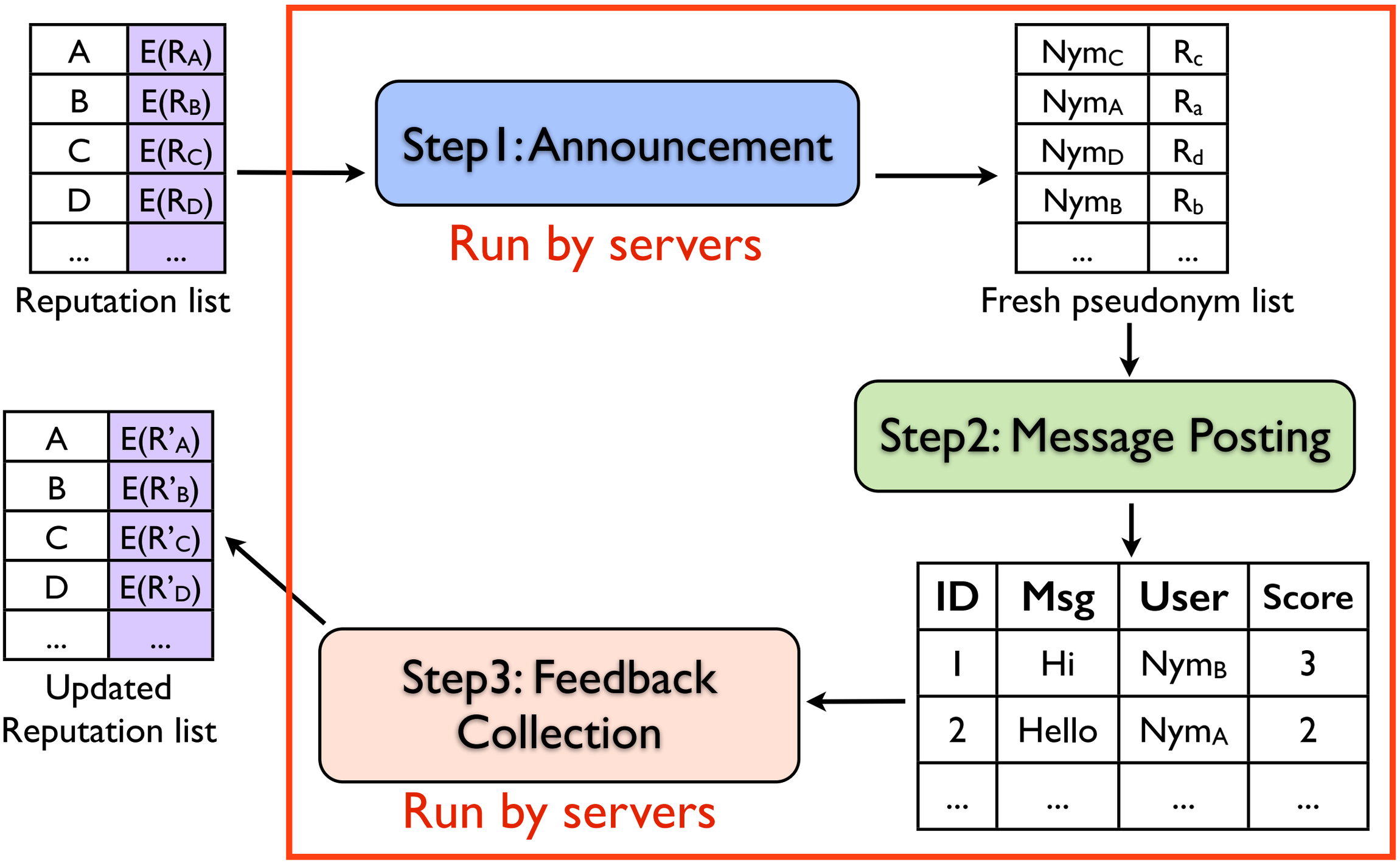
Three Steps in Each Round



Three Steps in Each Round

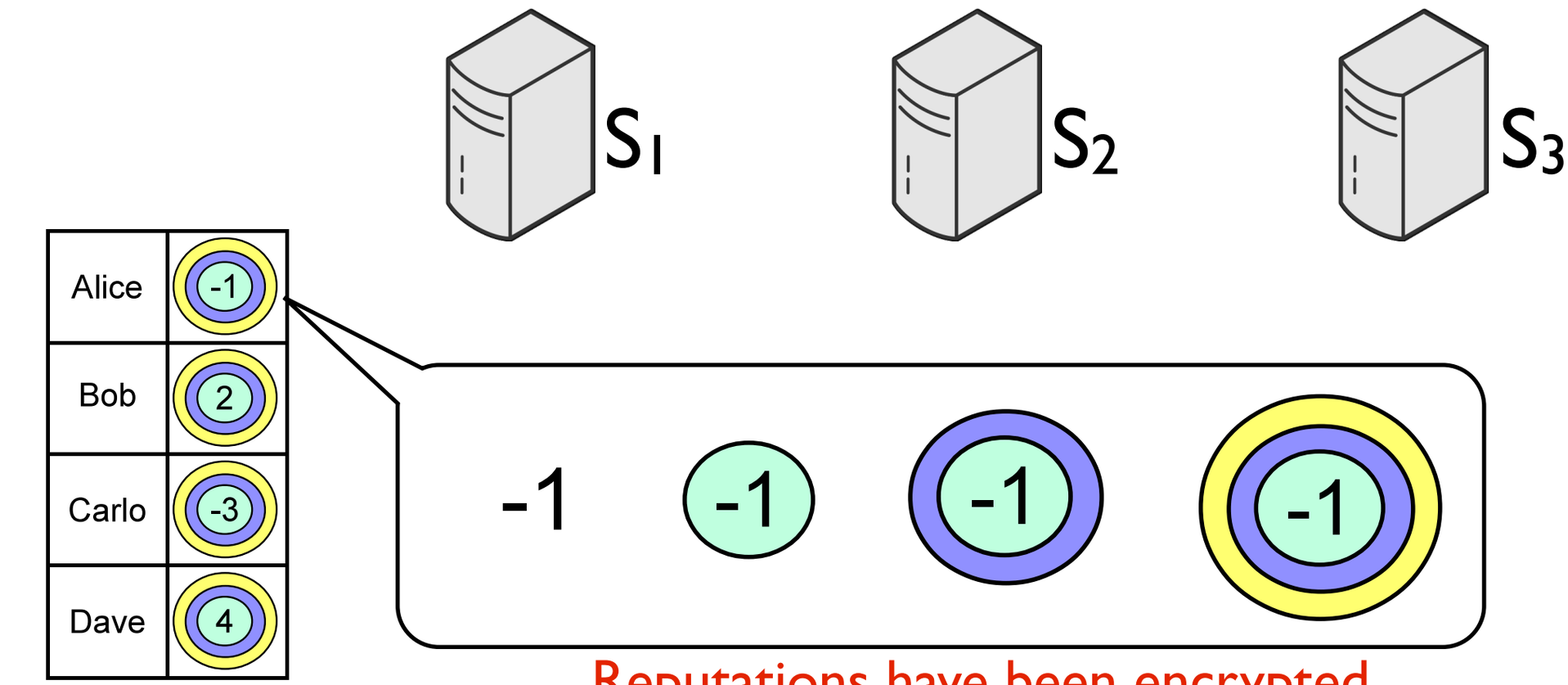


Three Steps in Each Round

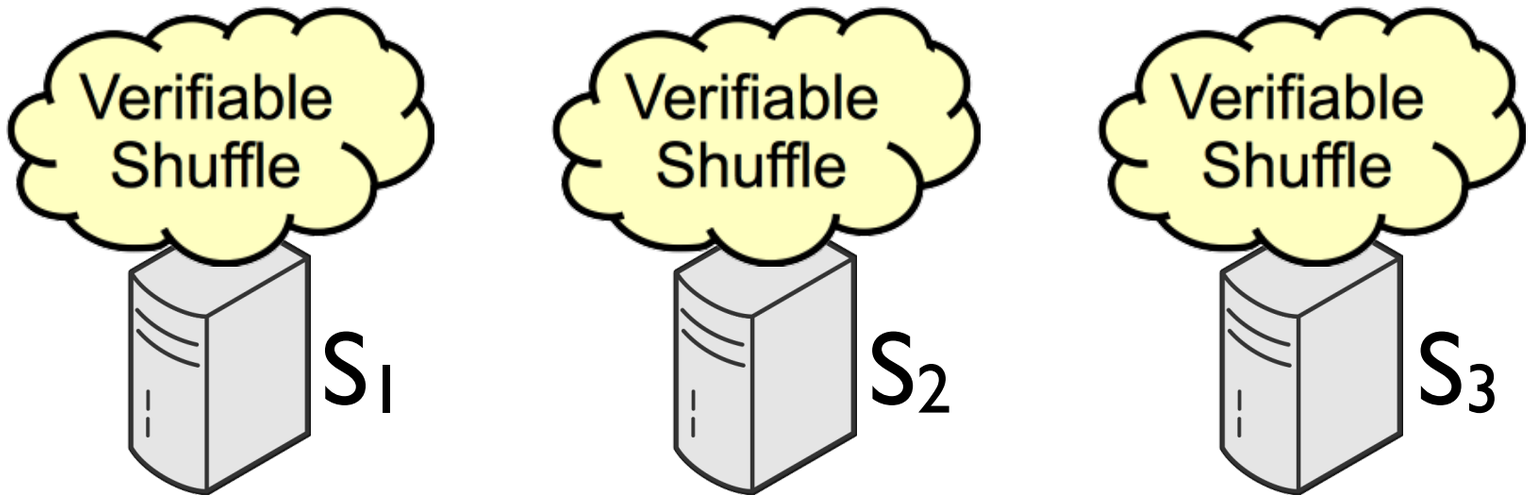


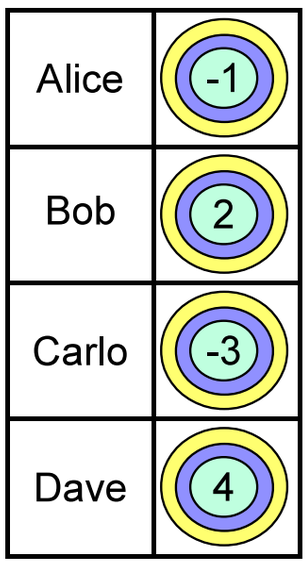
Step1: Announcement

Step1: Announcement



Step1: Announcement

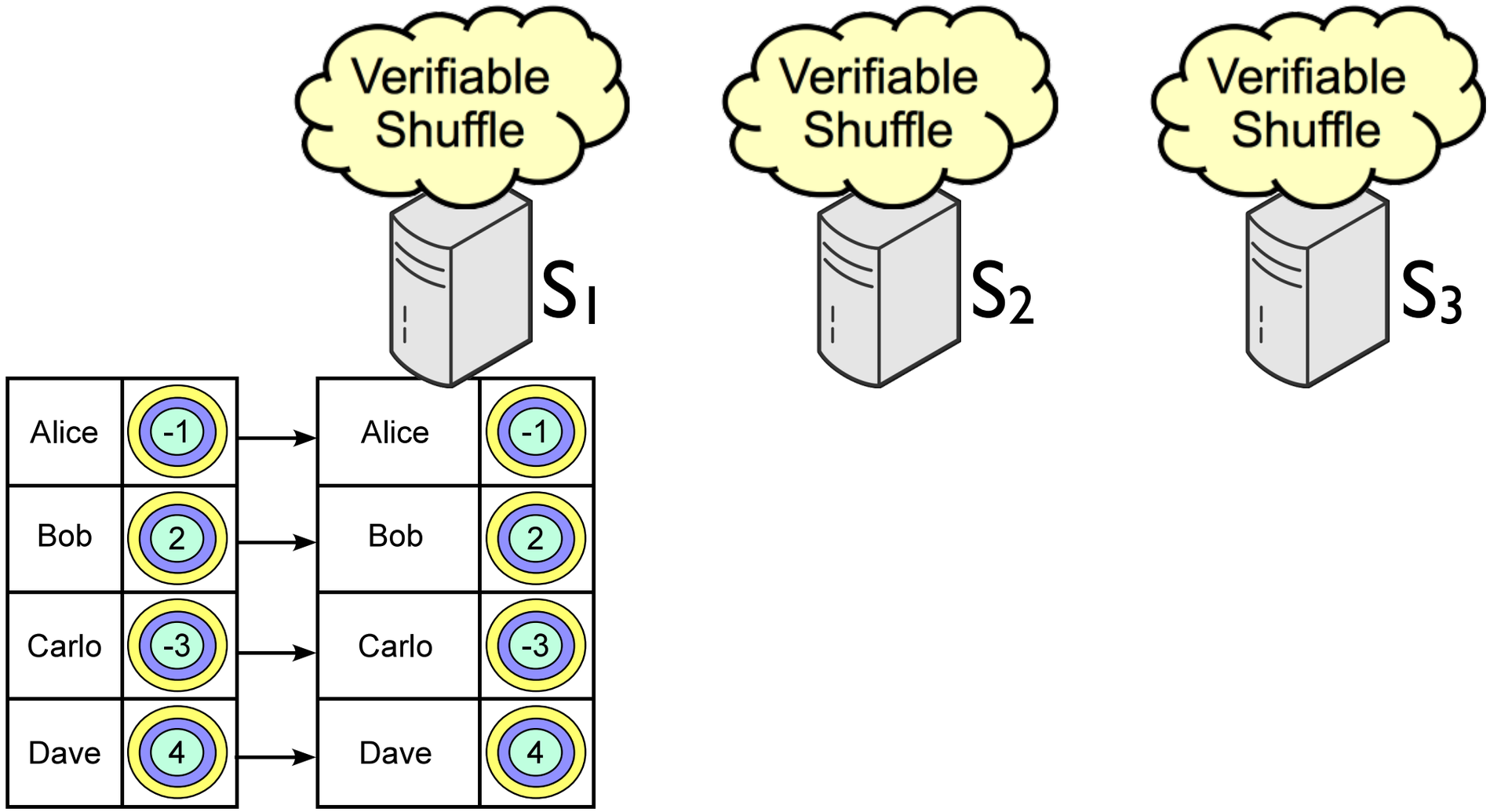




Reputation List

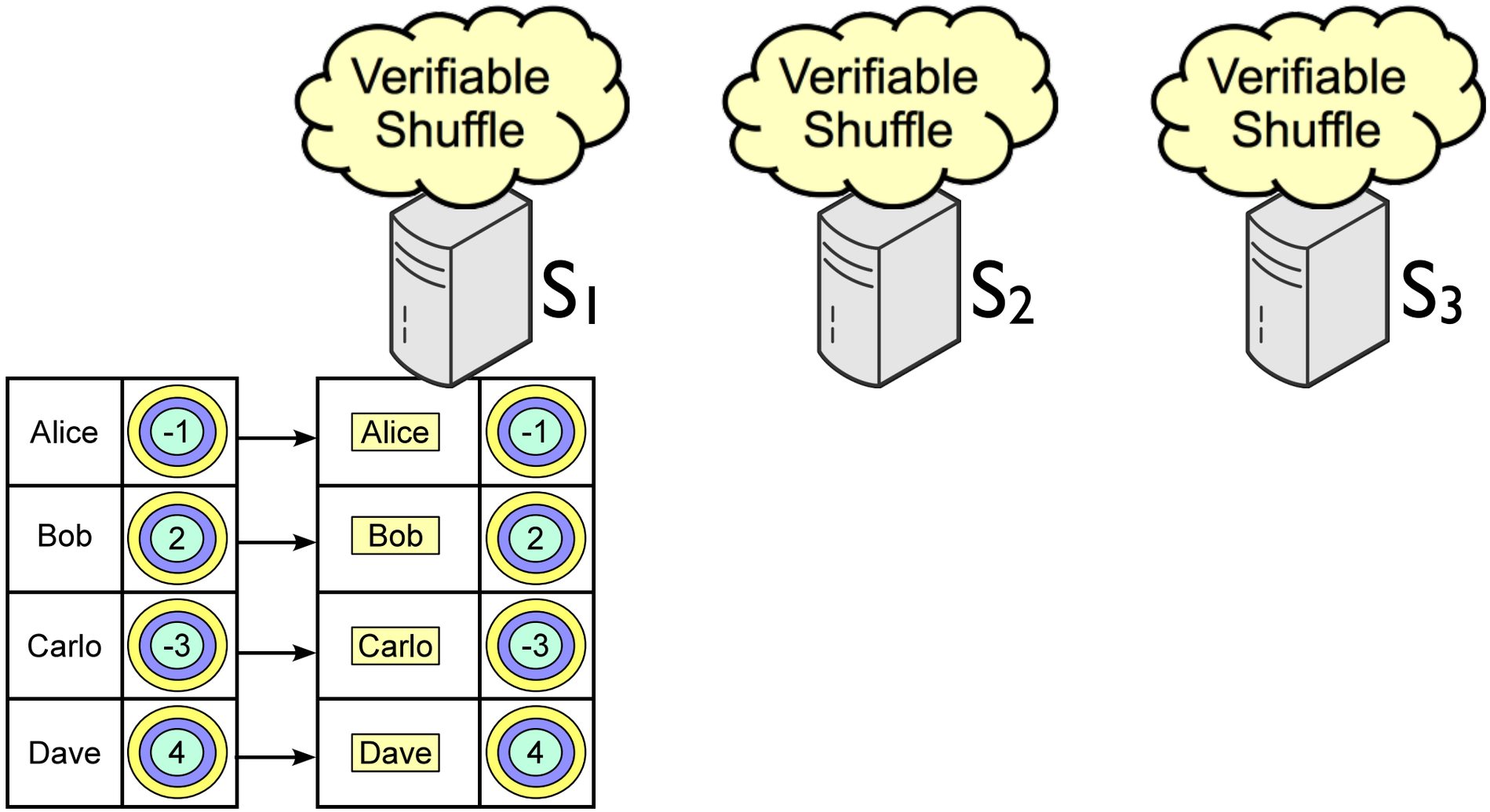
* C. Andrew Neff. A verifiable secret shuffle and its application to e-voting. In CCS'01.

Step1: Announcement



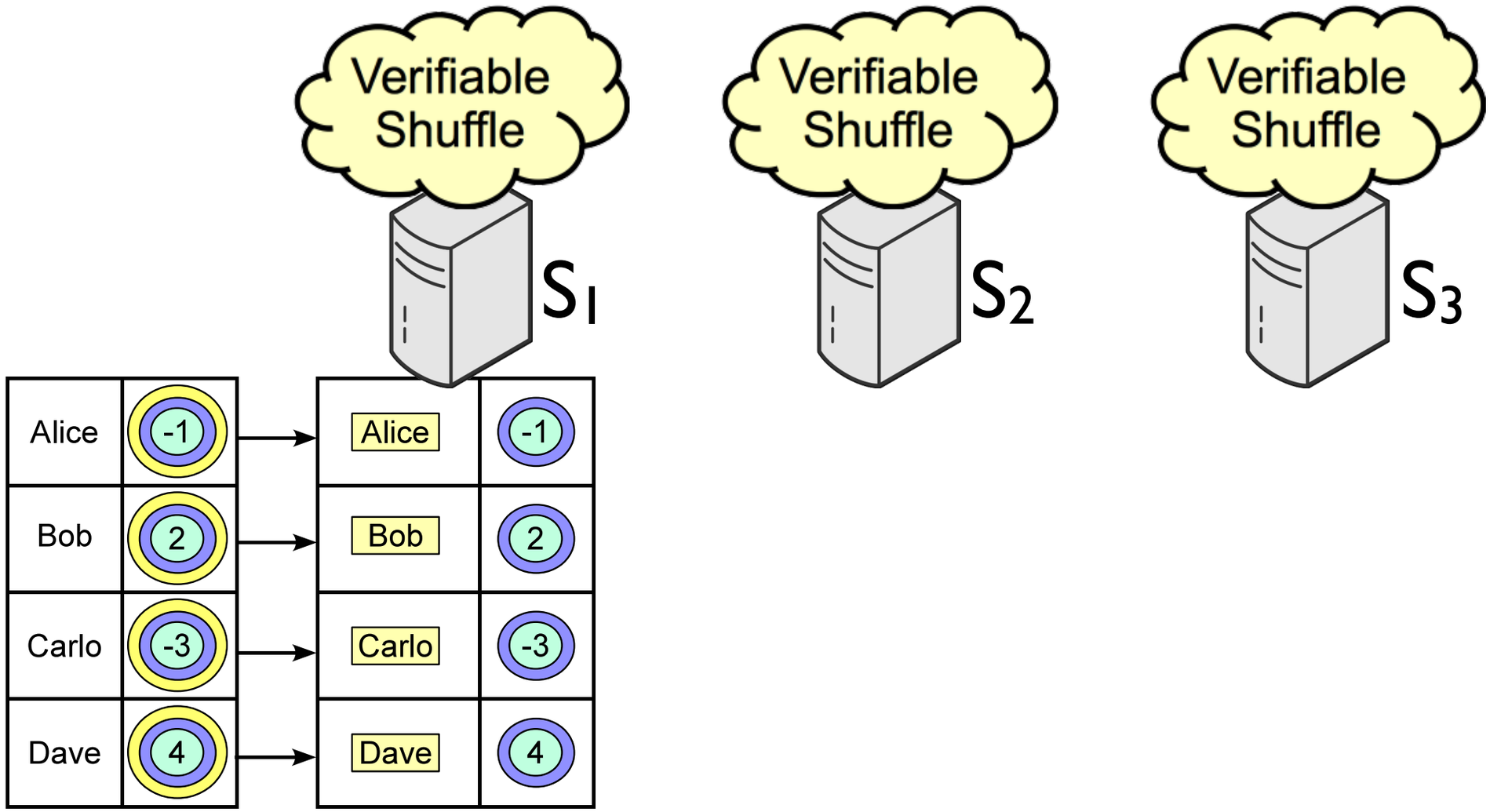
Reputation List

Step1: Announcement



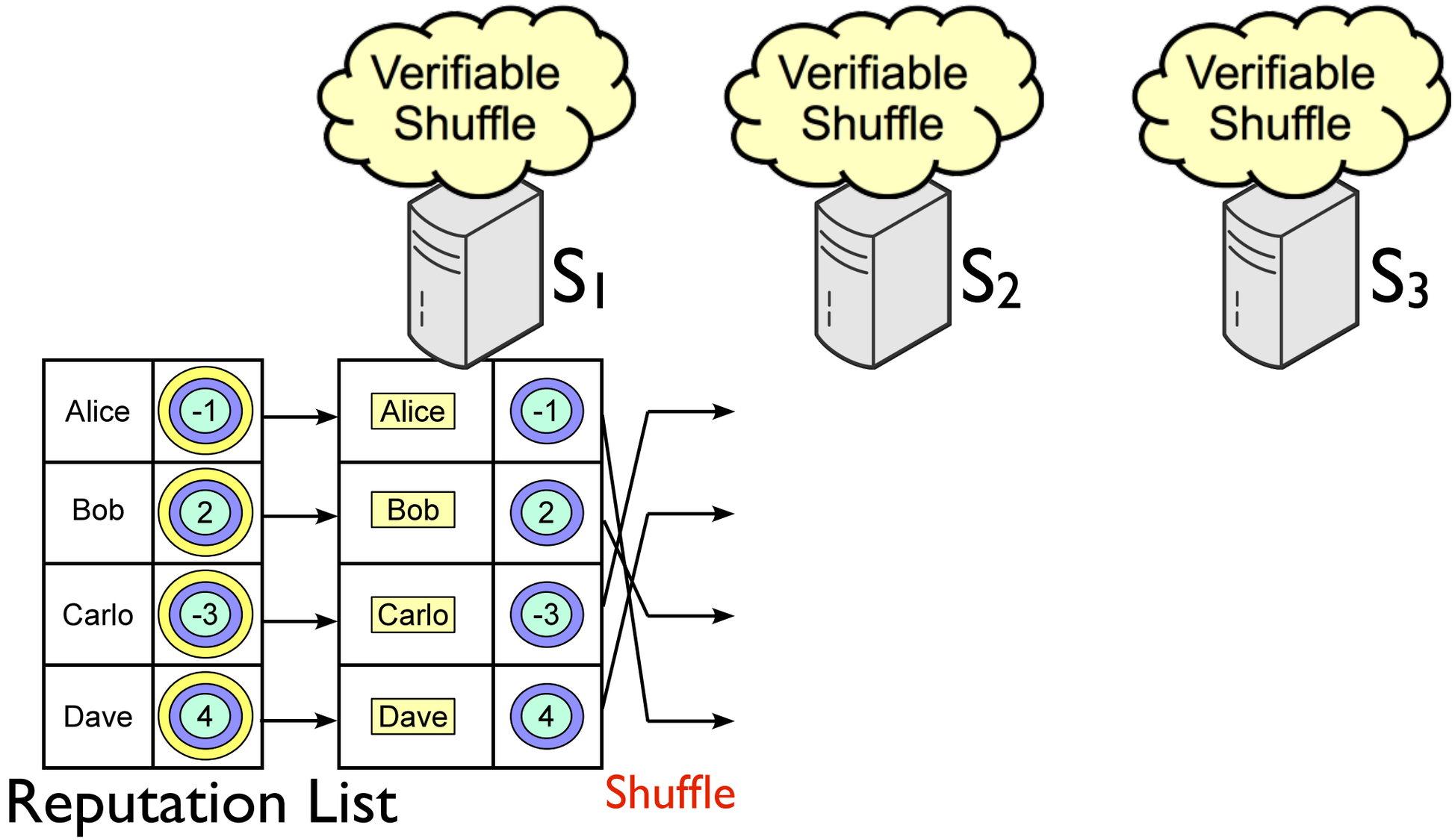
Reputation List

Step1: Announcement

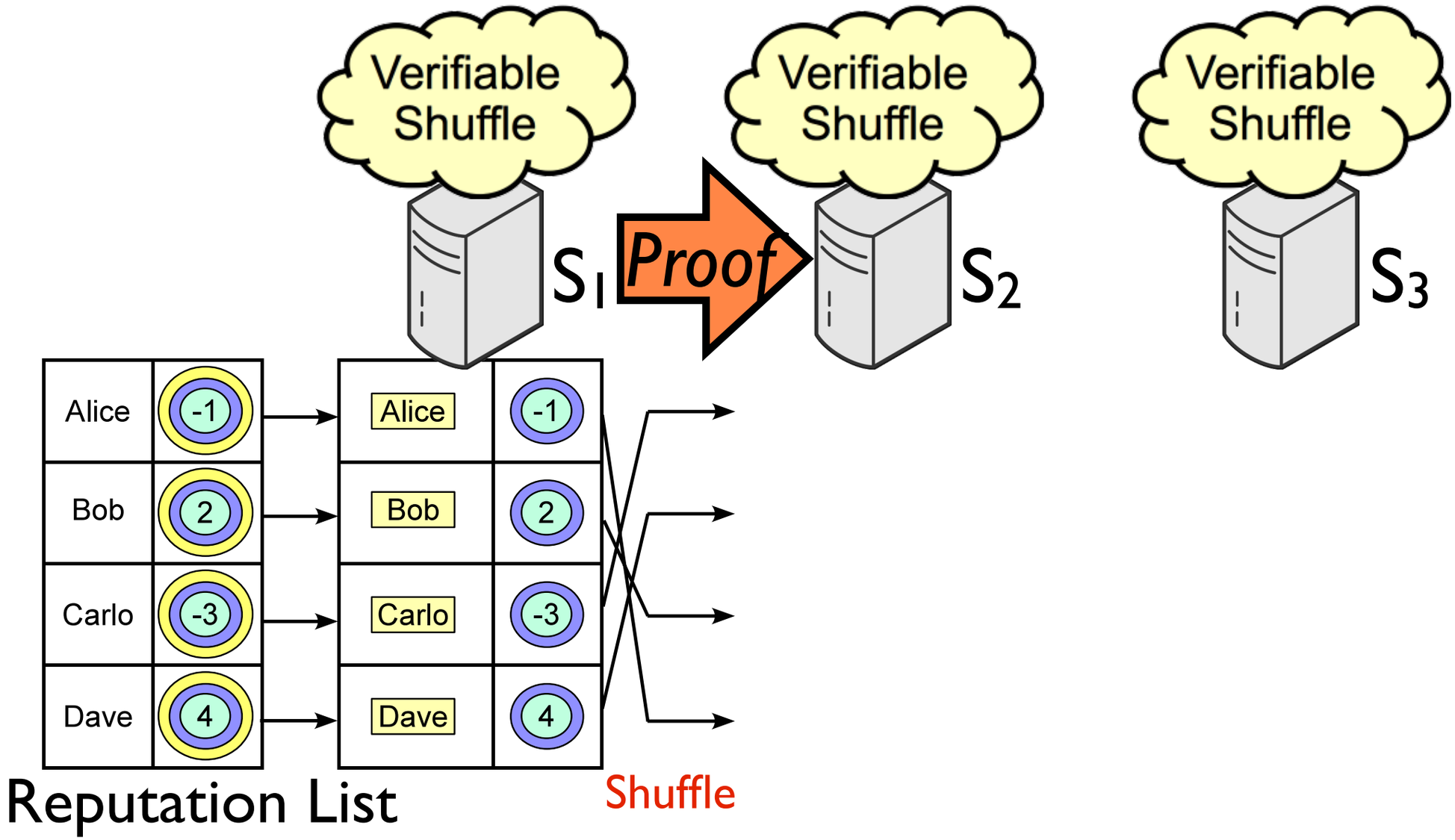


Reputation List

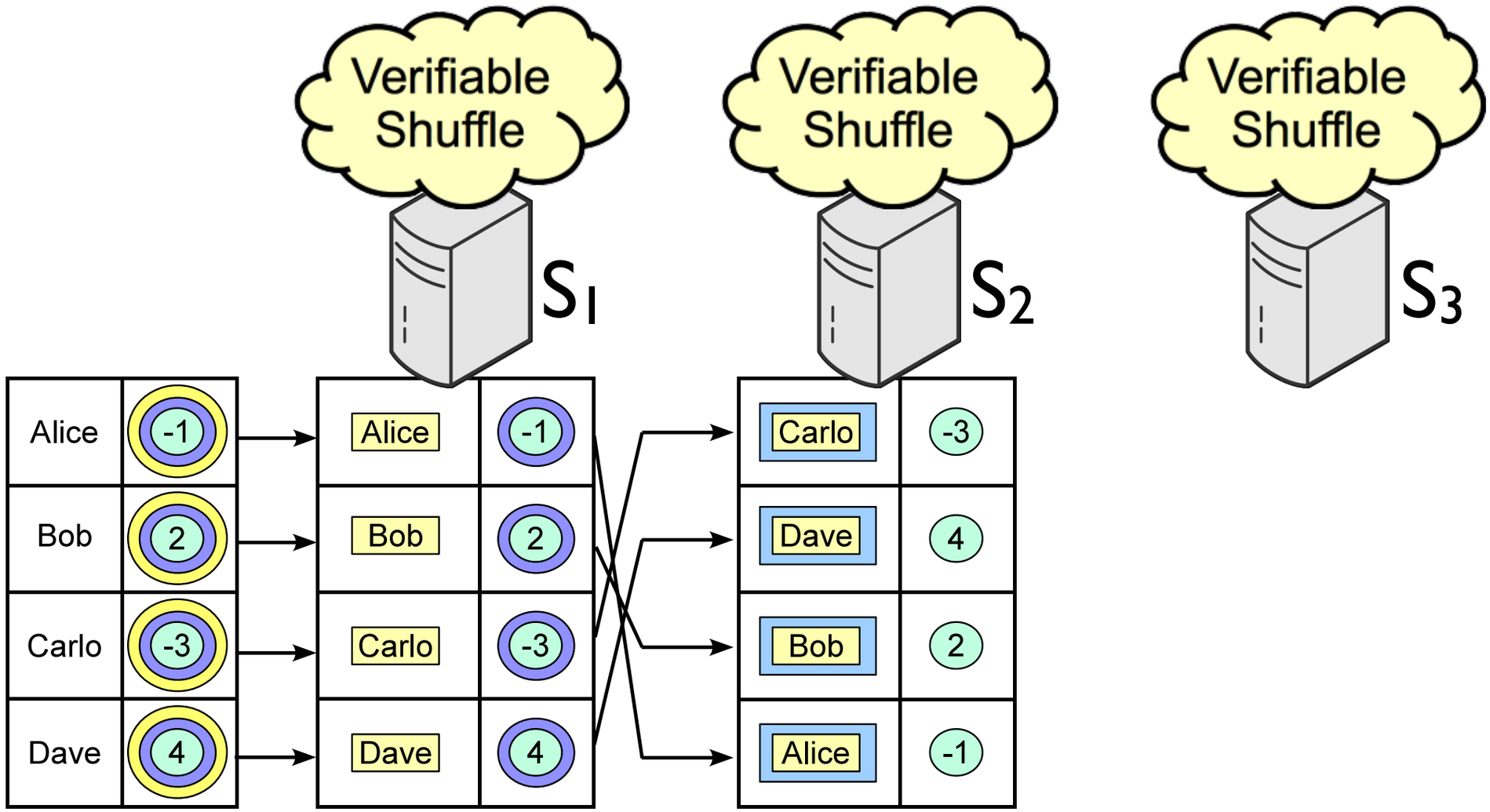
Step1: Announcement



Step1: Announcement

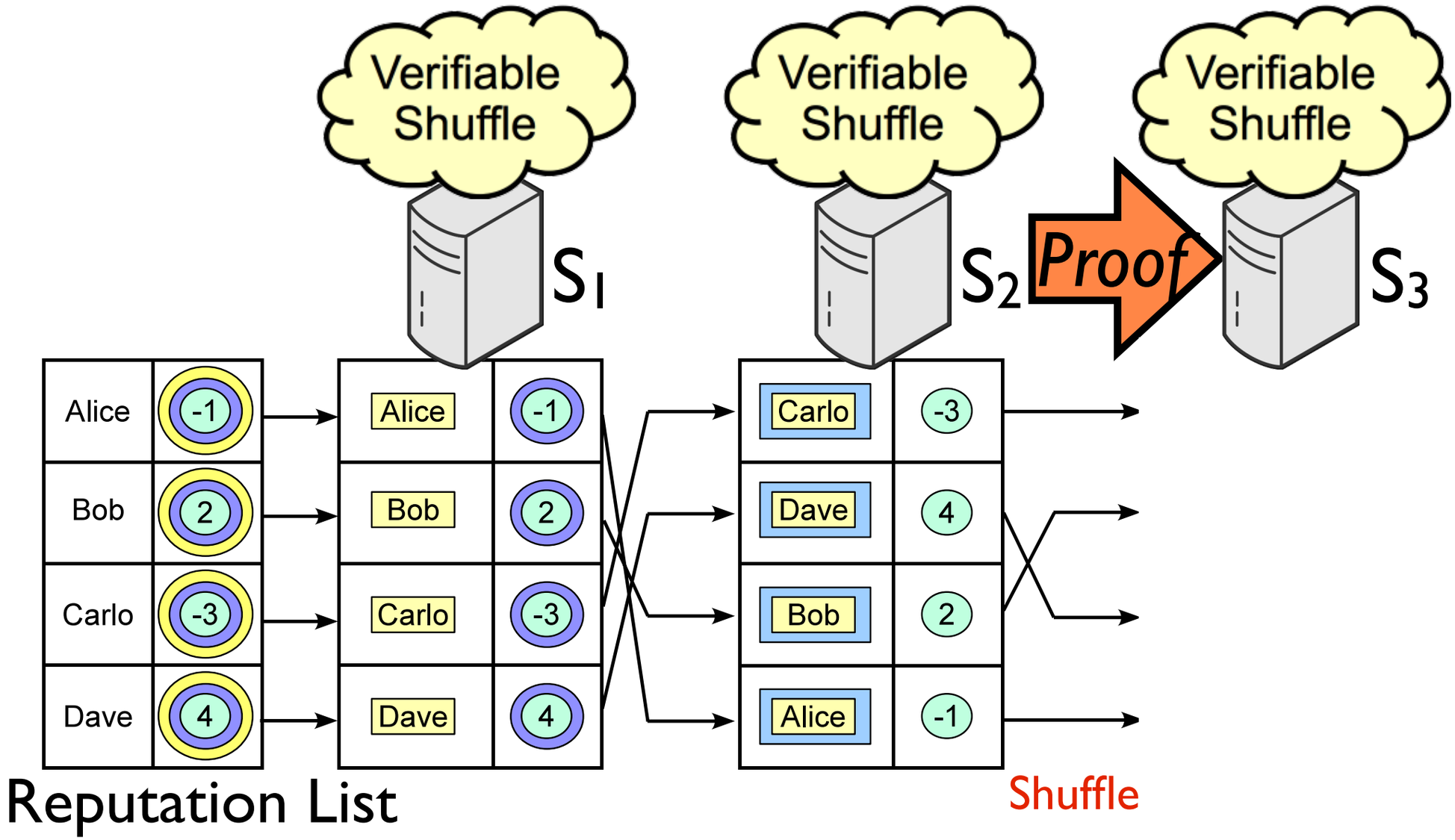


Step1: Announcement

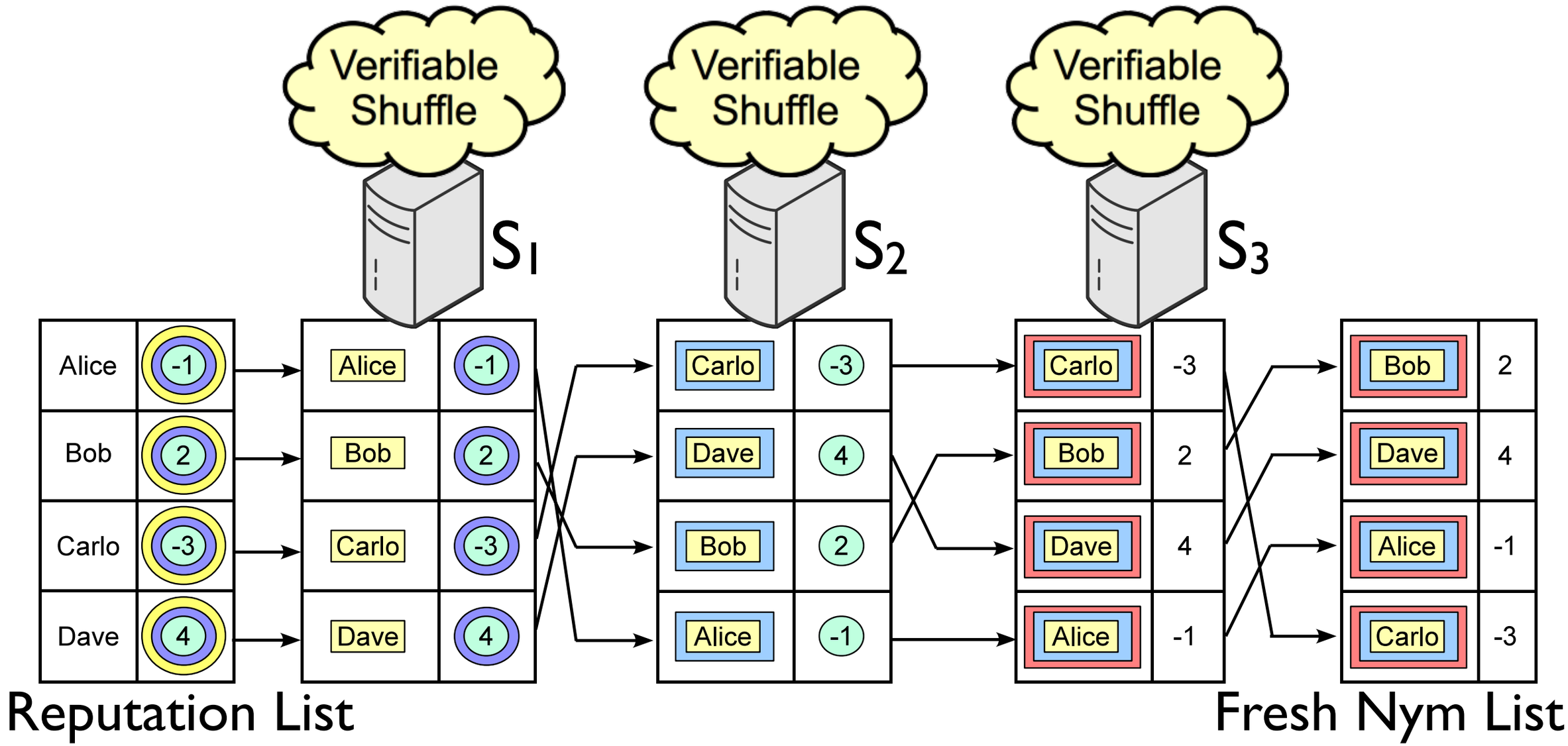


Reputation List

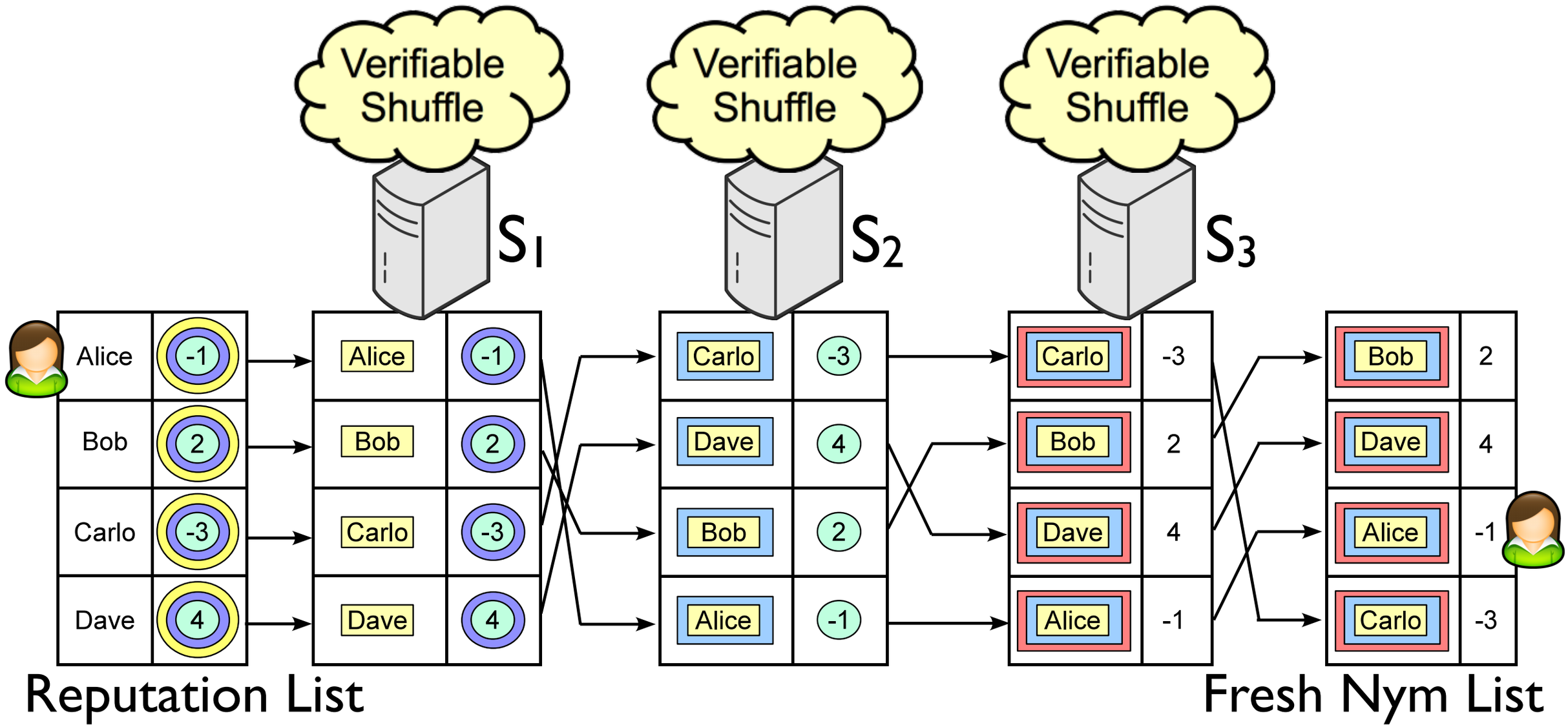
Step1: Announcement



Step1: Announcement



Step1: Announcement



Step2: Message Posting

Step2: Message Posting

Nym	Score
Nym_C	-2
Nym_A	2
Nym_D	-1
Nym_B	3
...	...

Fresh Nym List

Step2: Message Posting

Nym	Score
Nym_C	-2
Nym_A	2
Nym_D	-1
Nym_B	3
...	...

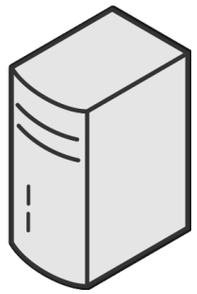
Fresh Nym List

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

Step2: Message Posting

Nym	Score
Nym_C	-2
Nym_A	2
Nym_D	-1
Nym_B	3
...	...

Fresh Nym List



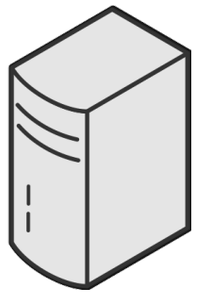
MsgID	Msg	User	Score
...	...	...	...

Bob

Step2: Message Posting

Nym	Score
Nym_C	-2
Nym_A	2
Nym_D	-1
Nym_B	3
...	...

Fresh Nym List



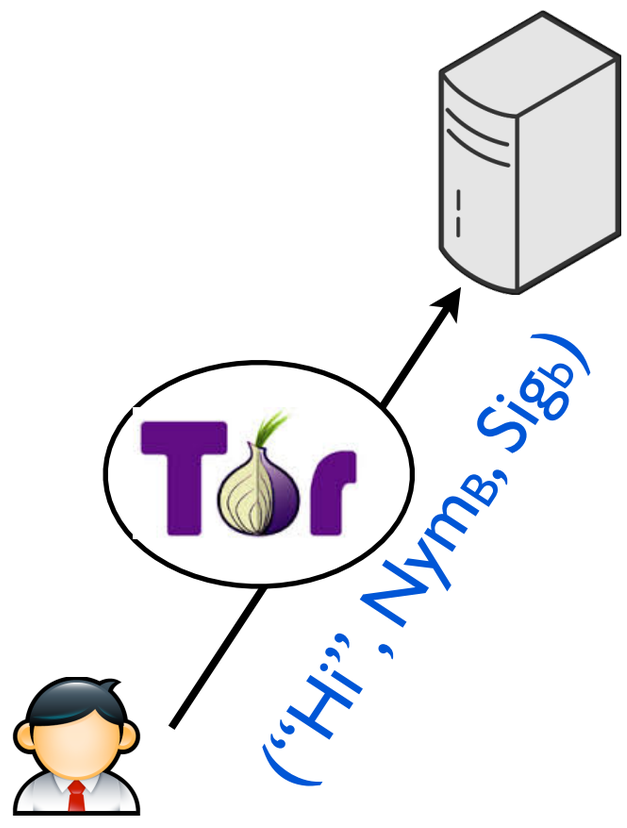
MsgID	Msg	User	Score
...	...	...	...

Bob ("Hi", Nym_B, Sig_b)

Step2: Message Posting

Nym	Score
Nym_C	-2
Nym_A	2
Nym_D	-1
Nym_B	3
…	…

Fresh Nym List

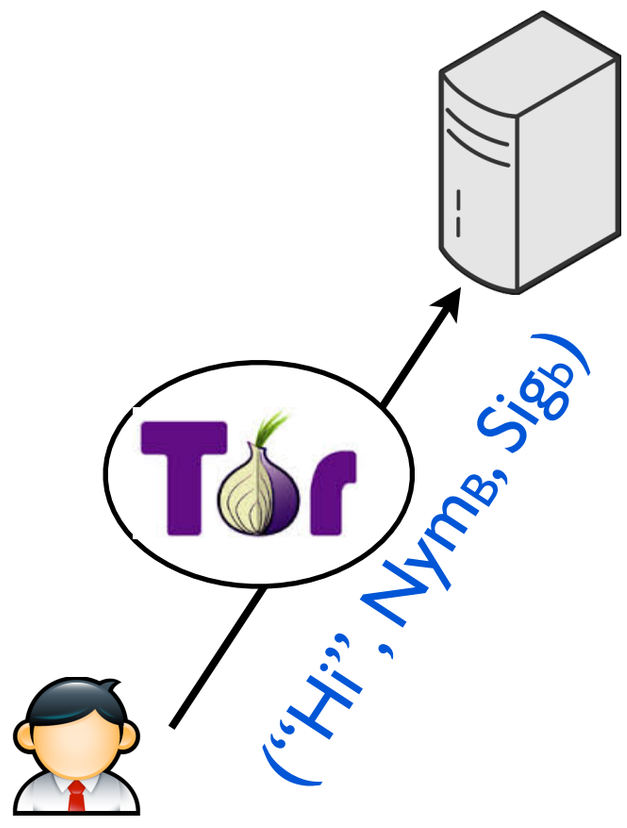


MsgID	Msg	User	Score
…	…	…	…

Step2: Message Posting

Nym	Score
Nym_C	-2
Nym_A	2
Nym_D	-1
Nym_B	3
…	…

Fresh Nym List

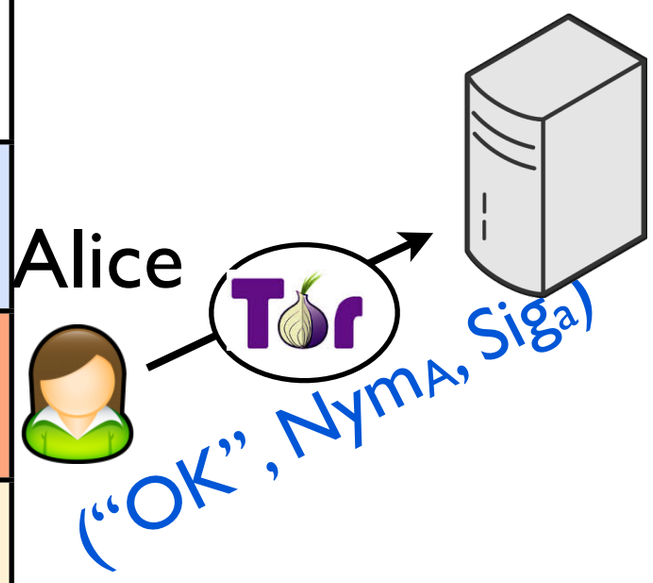


MsgID	Msg	User	Score
Msg1	Hi	Nym_B	3
…	…	…	…

Step2: Message Posting

Nym	Score
Nym_C	-2
Nym_A	2
Nym_D	-1
Nym_B	3
...	...

Fresh Nym List

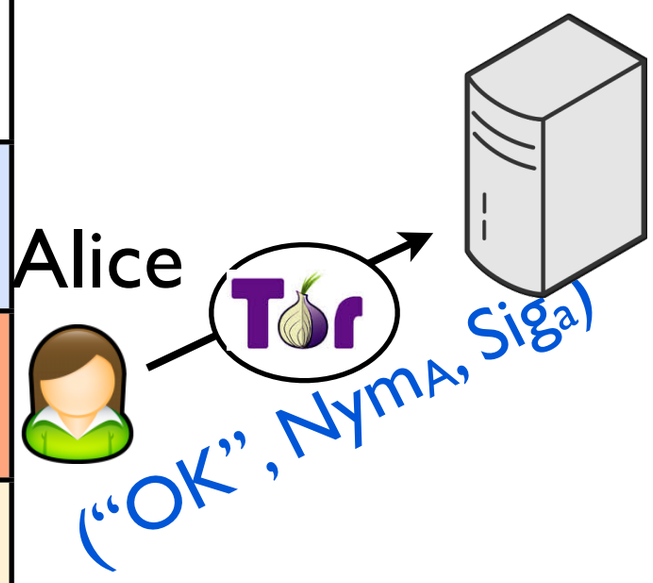


MsgID	Msg	User	Score
Msg1	Hi	Nym_B	3
...	...	...	...

Step2: Message Posting

Nym	Score
Nym_C	-2
Nym_A	2
Nym_D	-1
Nym_B	3
...	...

Fresh Nym List



MsgID	Msg	User	Score
Msg1	Hi	Nym_B	3
Msg2	OK	Nym_A	2
...	...	...	...

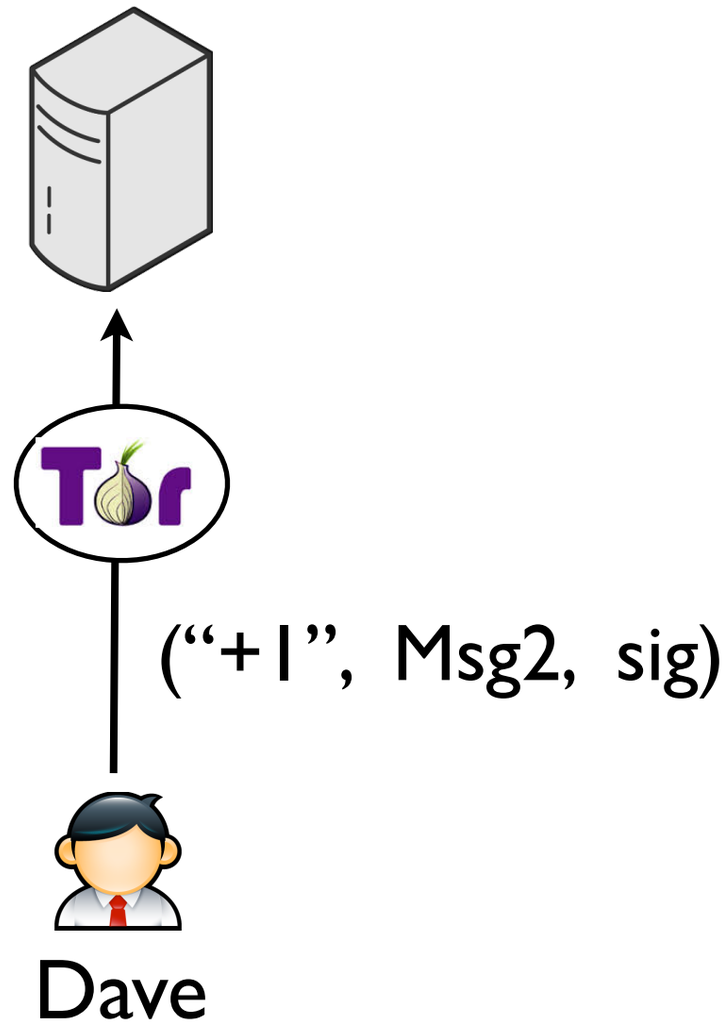
Step3: Feedback Collection

Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	3	
Msg2	Hello	Nym_A	2	
…	…	…	…	

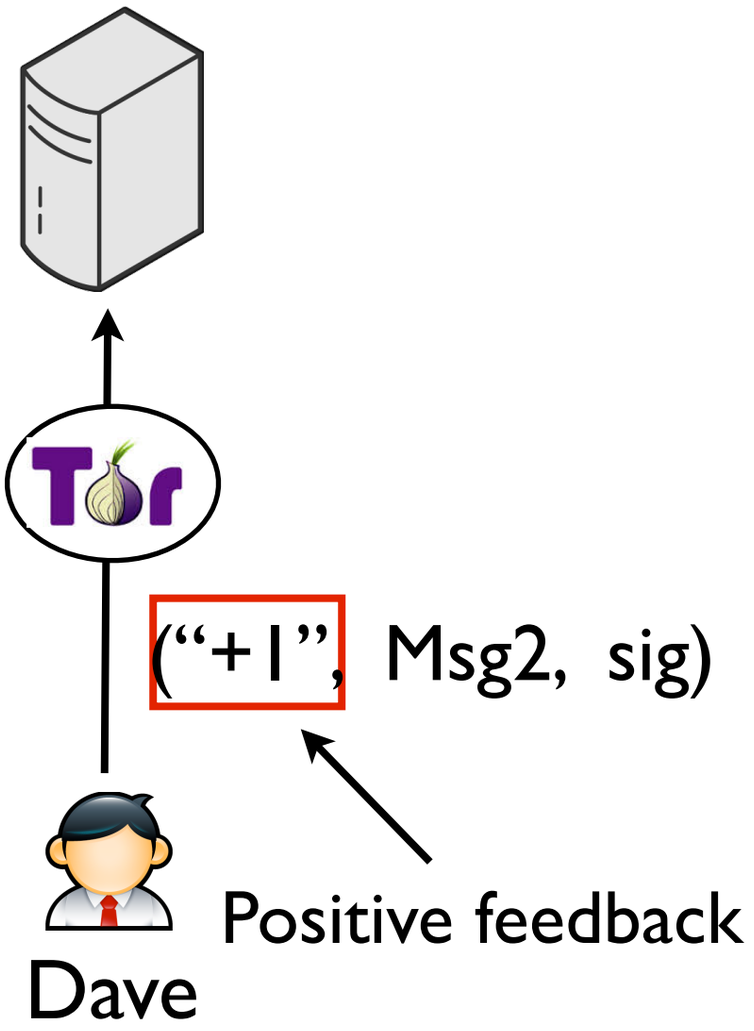
Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	3	
Msg2	Hello	Nym_A	2	
…	…	…	…	



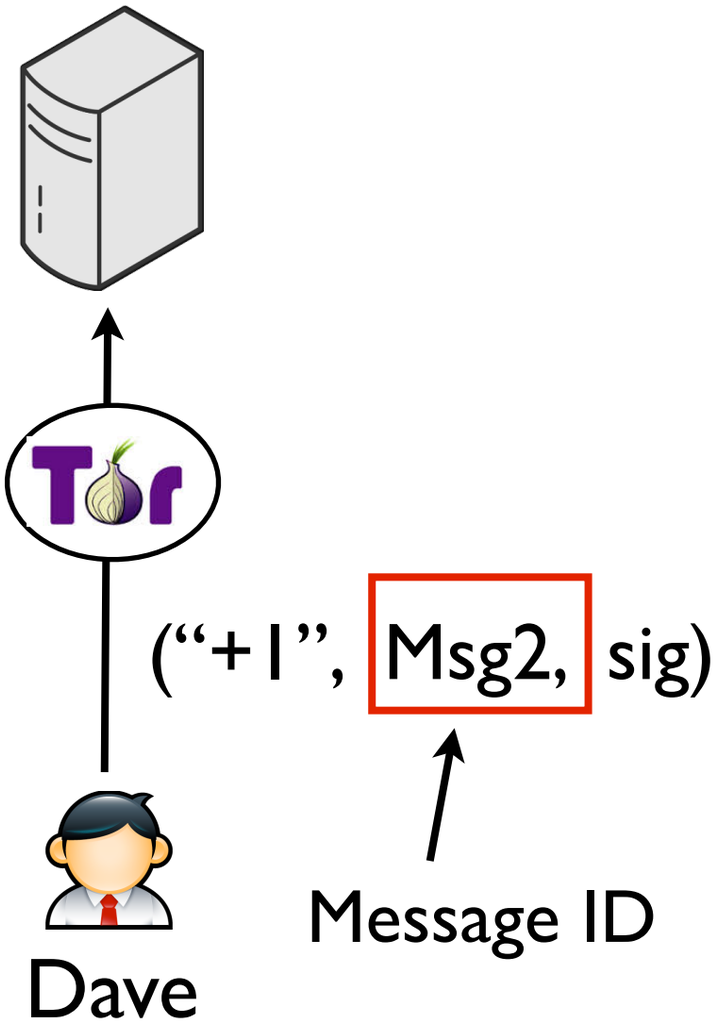
Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	3	
Msg2	Hello	Nym_A	2	
…	…	…	…	



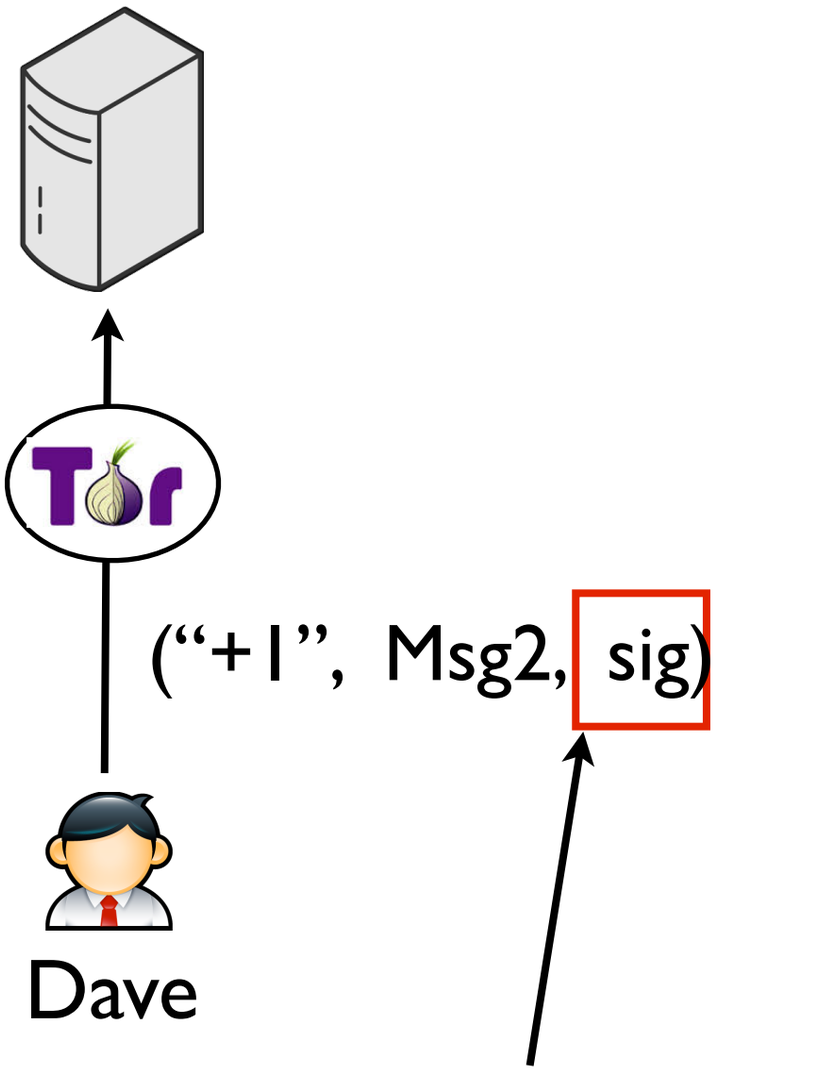
Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	3	
Msg2	Hello	Nym_A	2	
…	…	…	…	

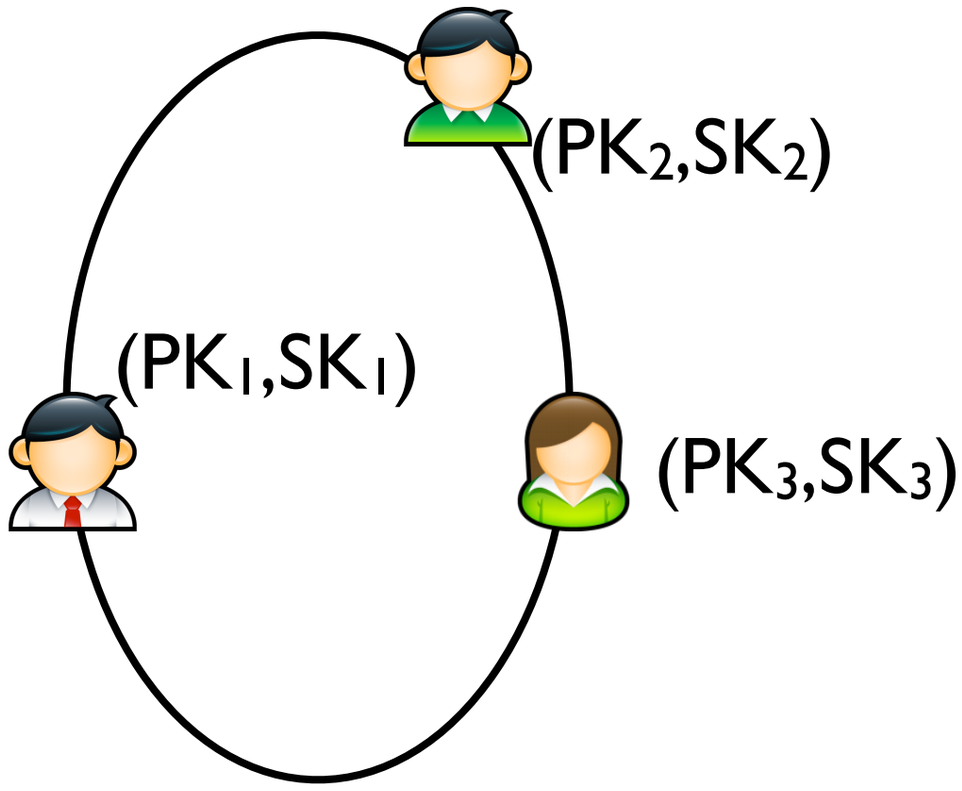


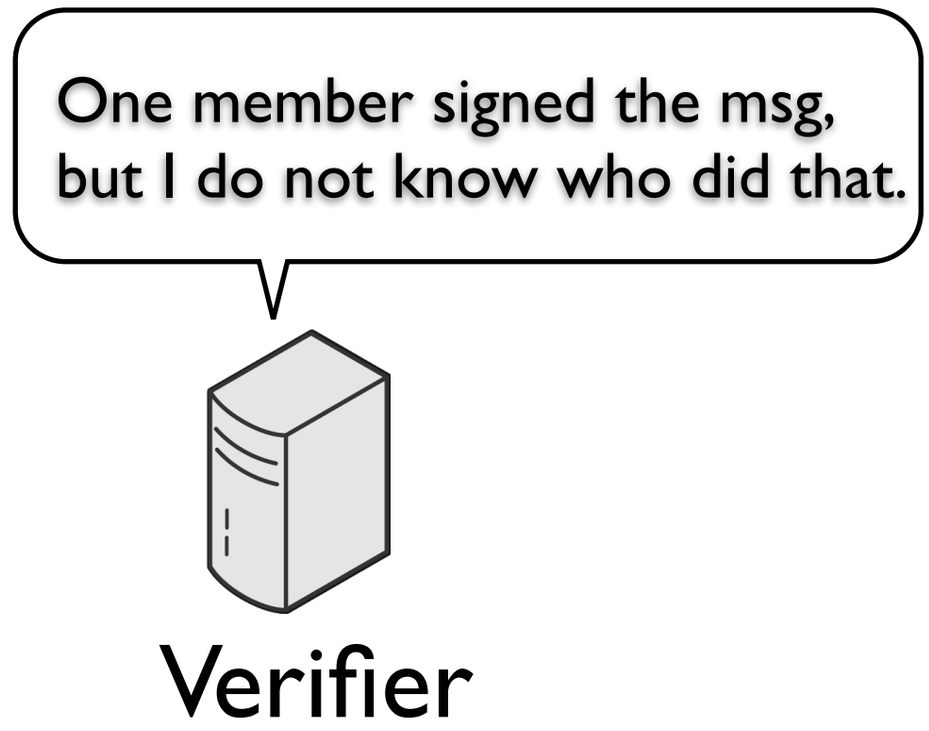
Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	3	
Msg2	Hello	Nym_A	2	
…	…	…	…	



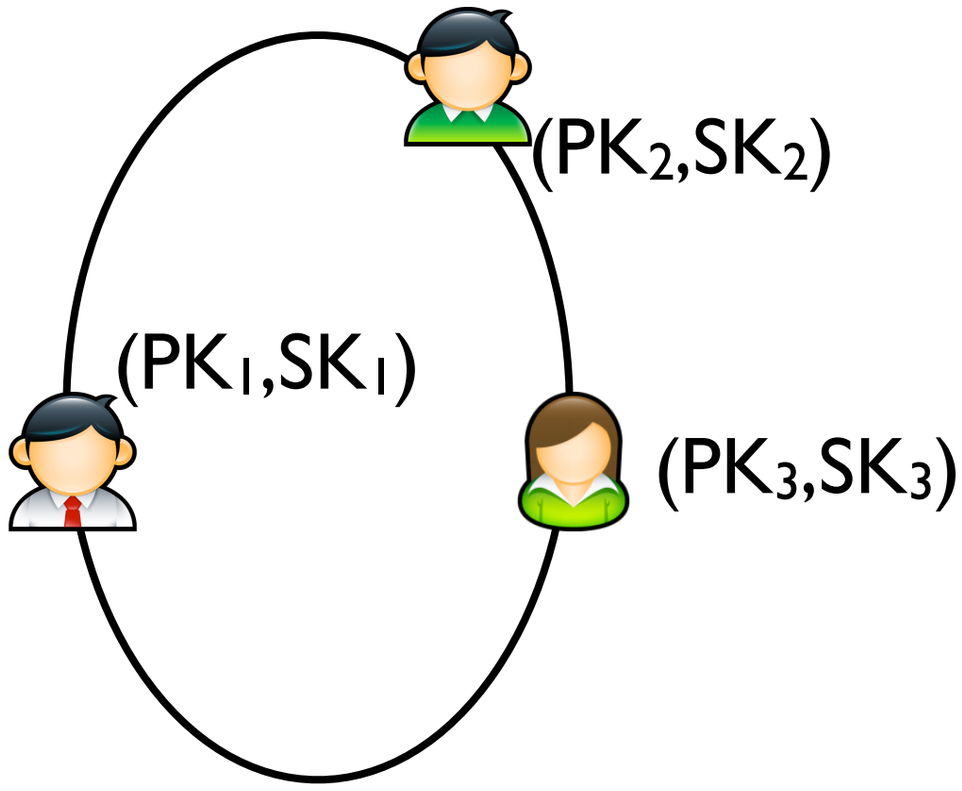
Linkable Ring Signature (LRS)

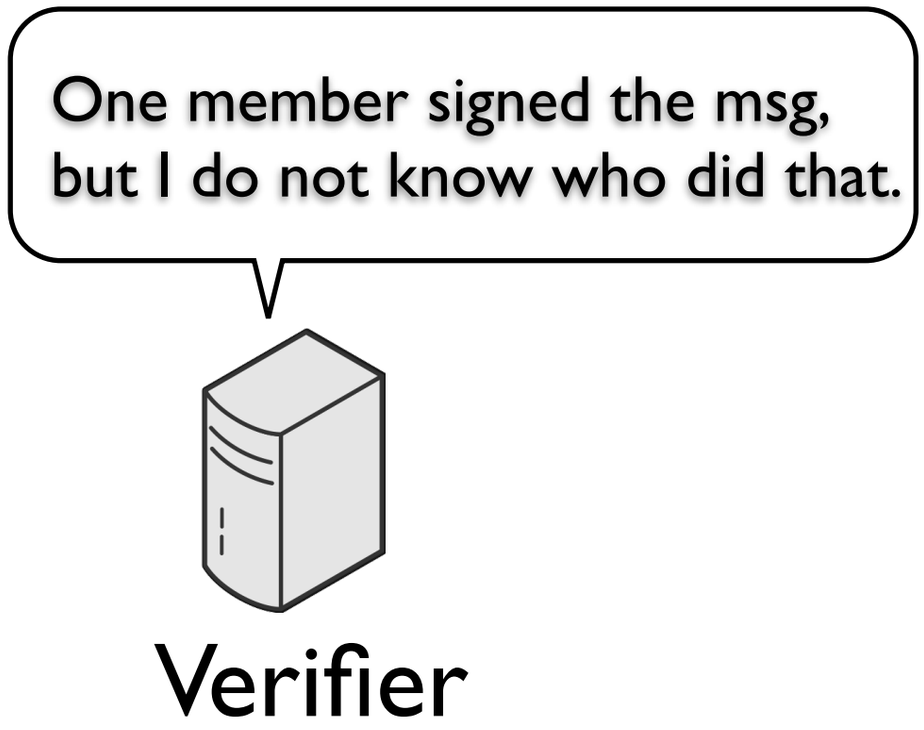




* Liu et al. Linkable ring signatures: Security models and new schemes. In ICCSA'05.

Linkable Ring Signature (LRS)

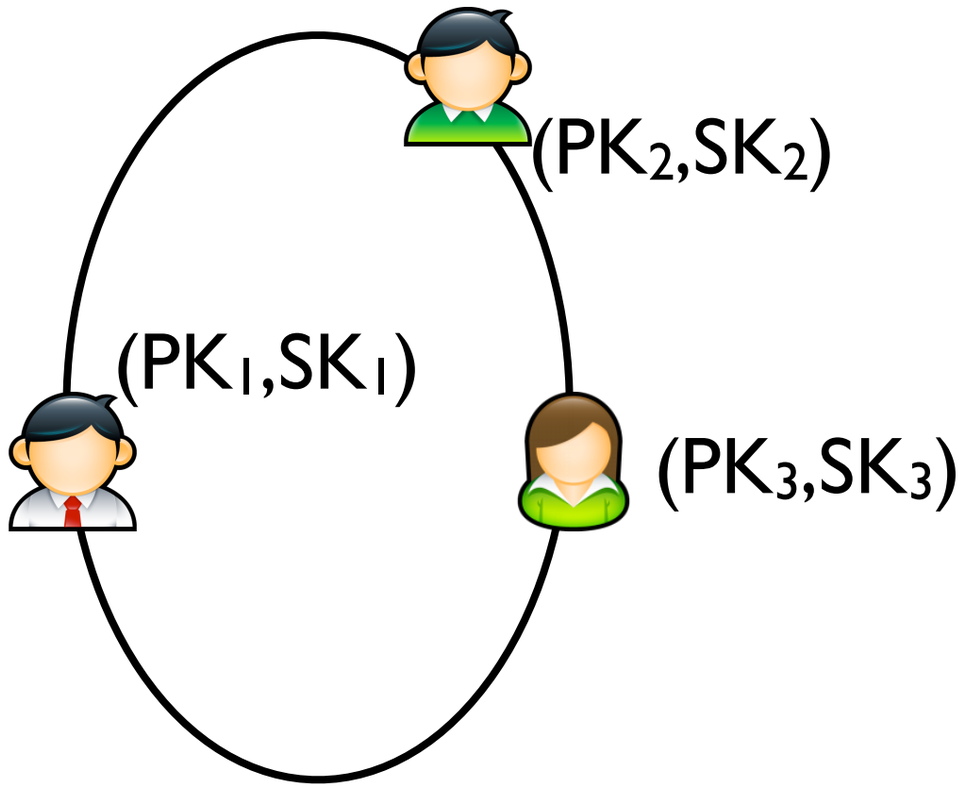


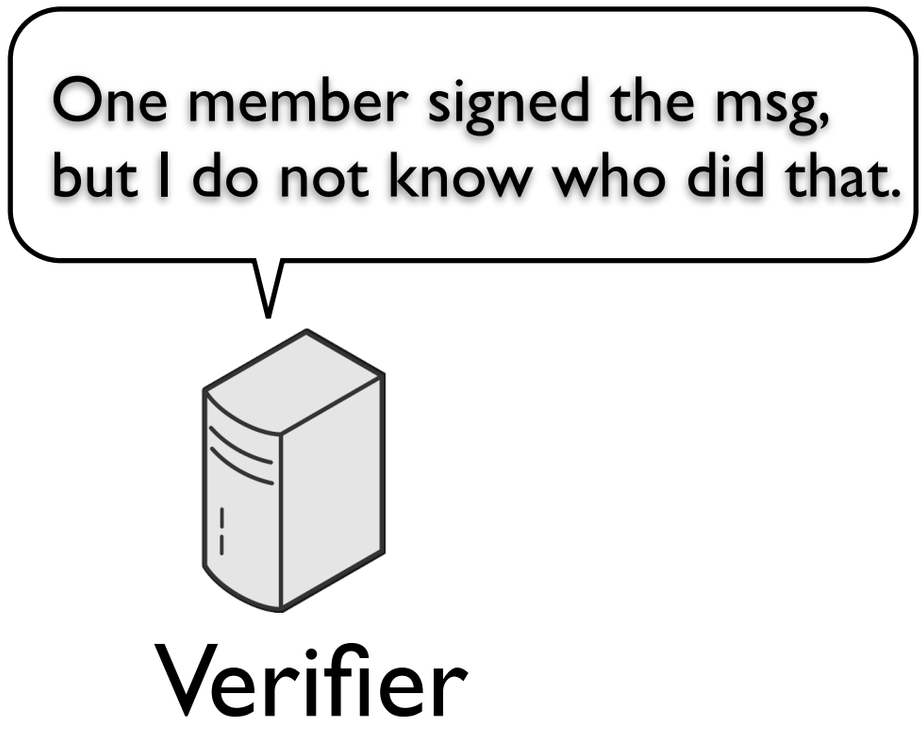


- LRS can hide voter's pseudonym

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

Linkable Ring Signature (LRS)

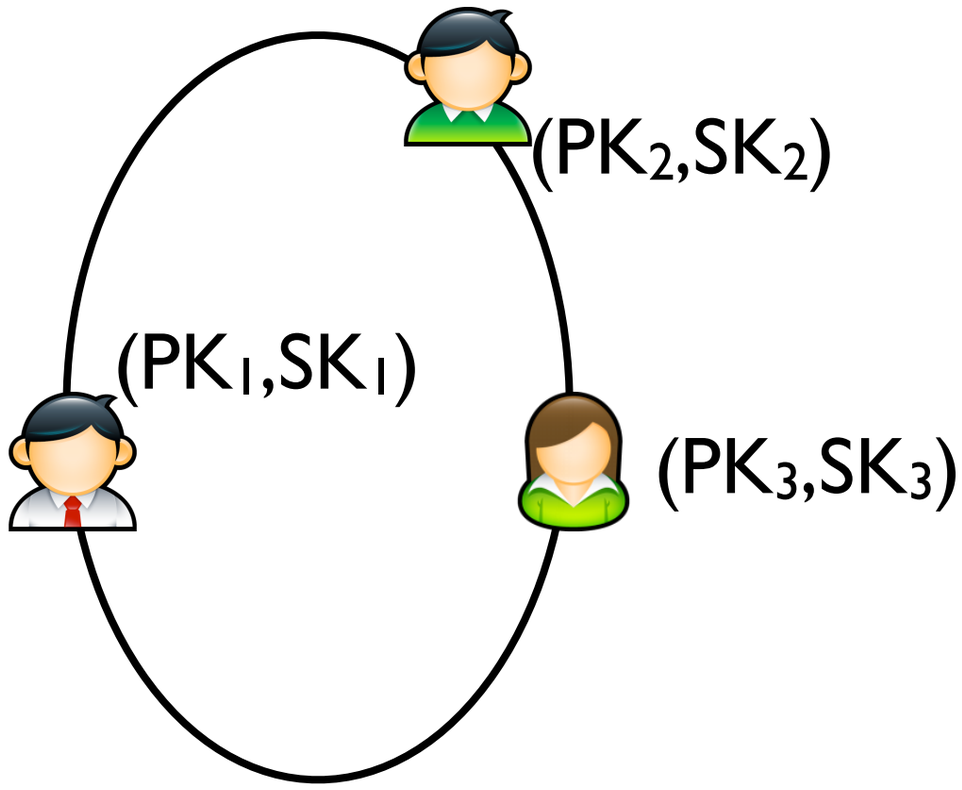


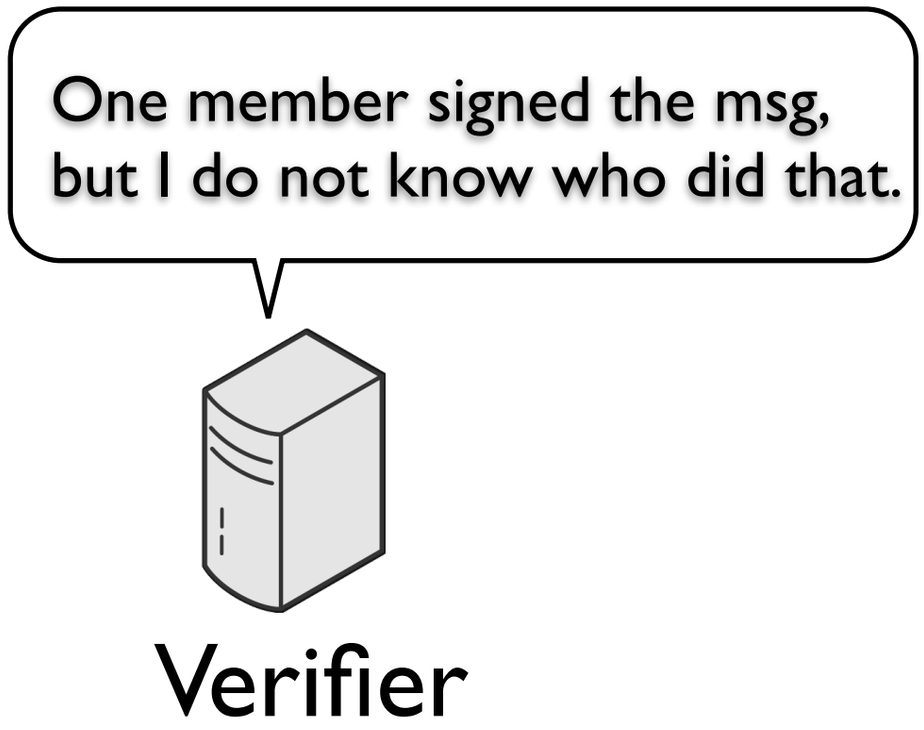


- LRS can hide voter's pseudonym
- LRS can avoid duplicate votes

* 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_B	3	Like: 2 Dislike: 1
Msg2	Hello	Nym_A	2	Like: 1
…	…	…	…	

Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	3	Like: 2 Dislike: 1
Msg2	Hello	Nym_A	2	Like: 1
...	...	...	...	

AnonRep supports diverse reputation algorithms

Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	3	Like: 2 Dislike: 1
Msg2	Hello	Nym_A	2	Like: 1
…	…	…	…	

3+2-1=4

2+1=3

Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	4	Like: 2 Dislike: 1
Msg2	Hello	Nym_A	3	Like: 1
…	…	…	…	

3+2-1=4

2+1=3

Nym_B's reputation becomes 4

Nym_A's reputation becomes 3

Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	4	Like: 2 Dislike: 1
Msg2	Hello	Nym_A	3	Like: 1
…	…	…	…	

3+2-1=4

2+1=3

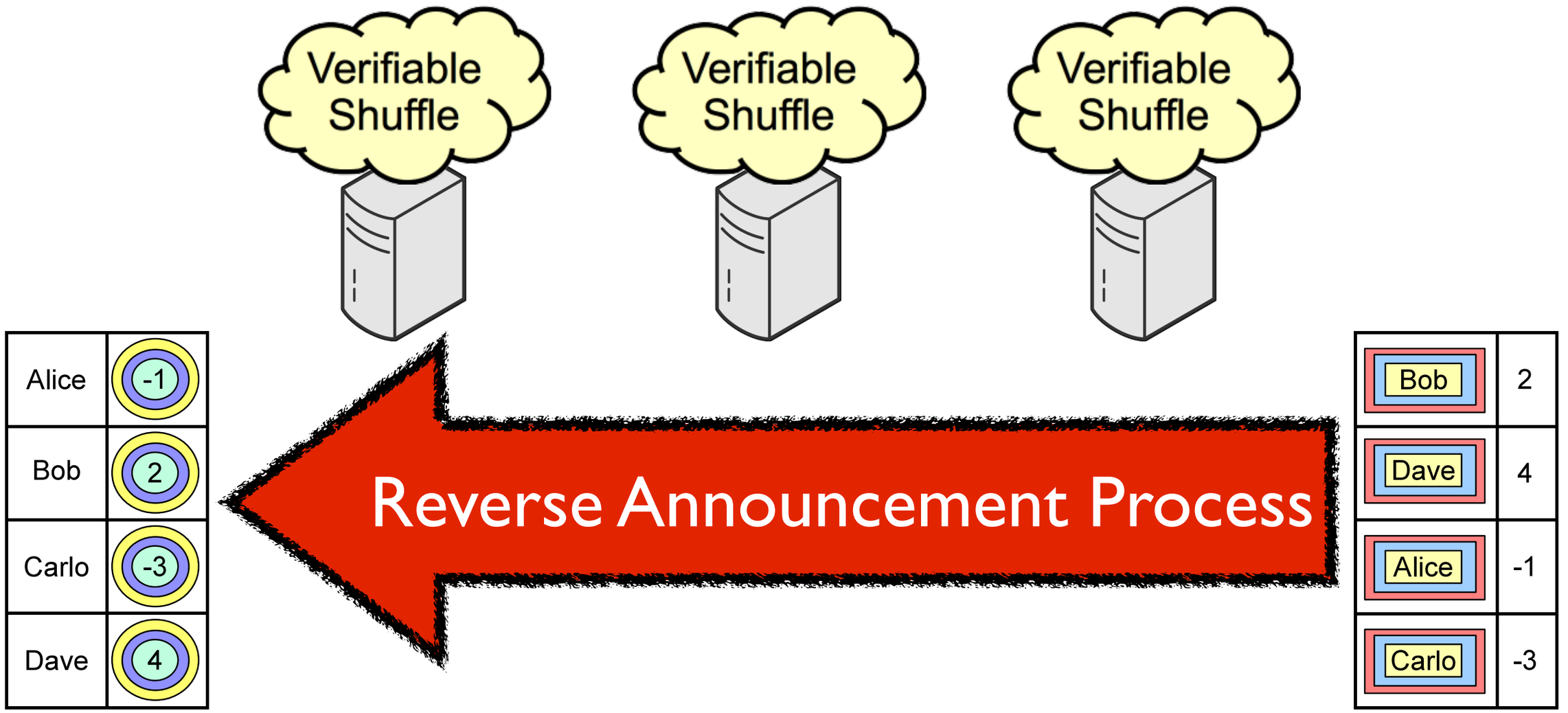
Fresh Nym list with updated reputation

Step3: Feedback Collection

Bob	2
Dave	4
Alice	-1
Carlo	-3

Updated Fresh Nym List

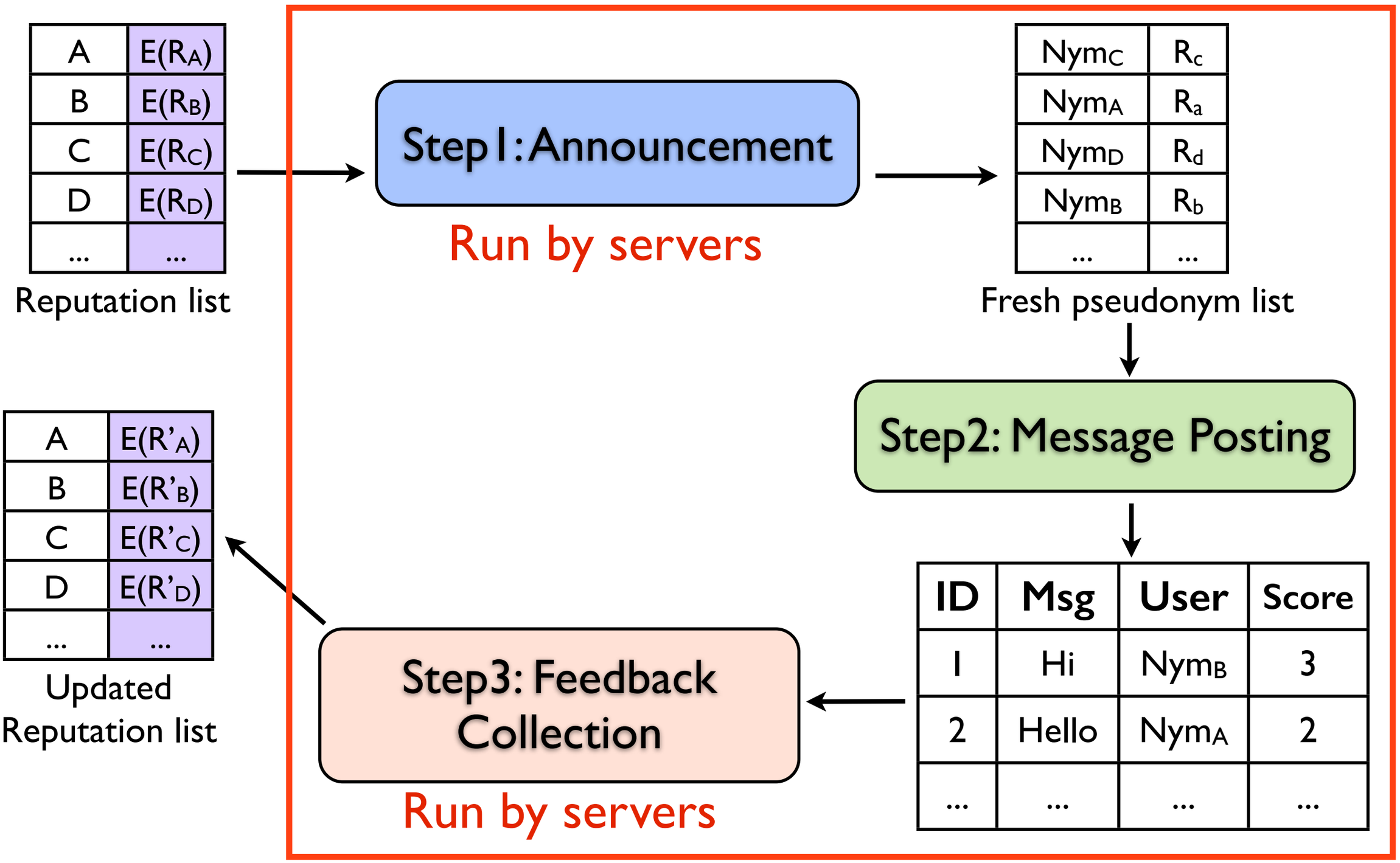
Step3: Feedback Collection



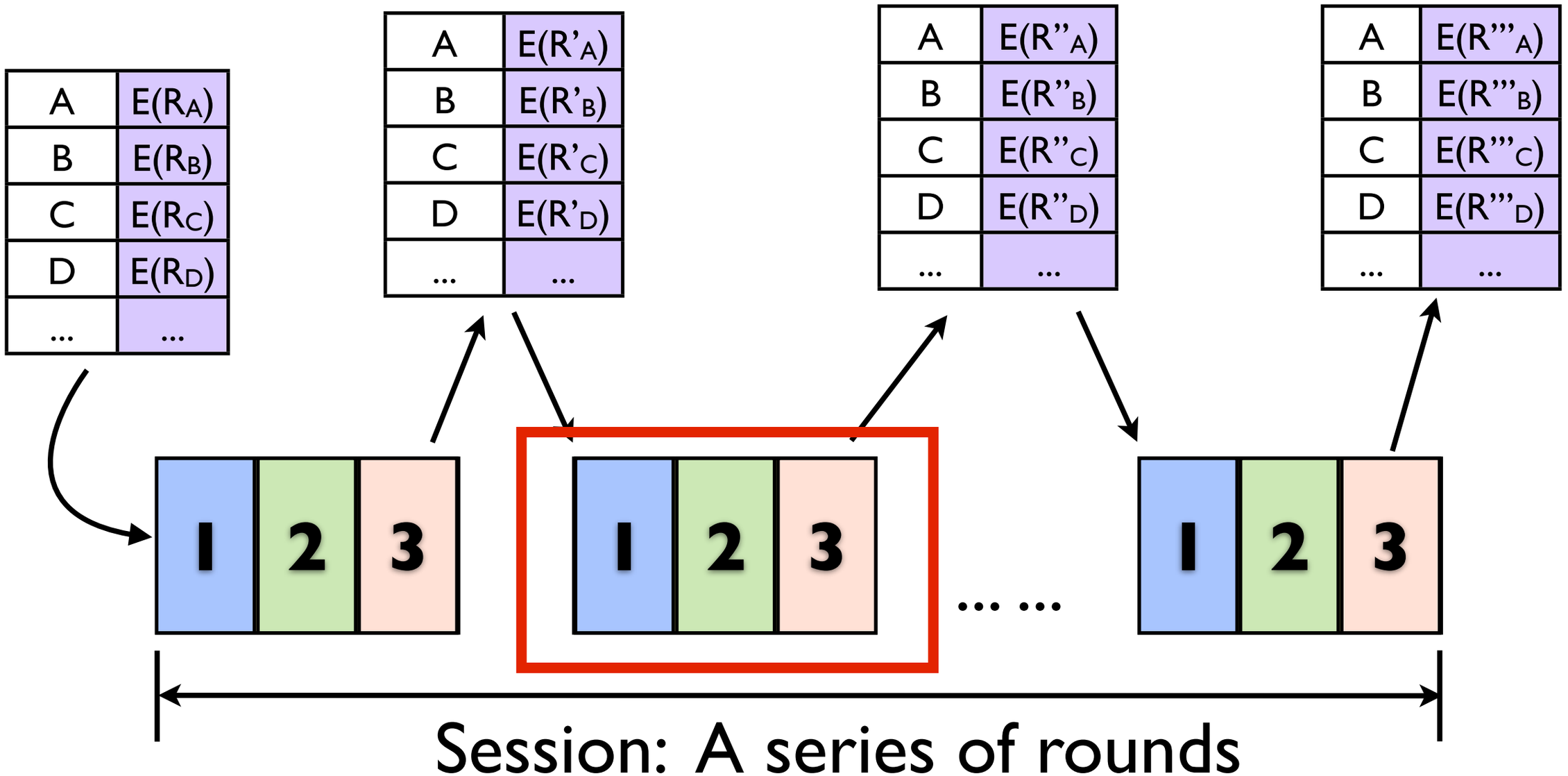
Updated Reputation List

Updated Fresh Nym List

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 like: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.

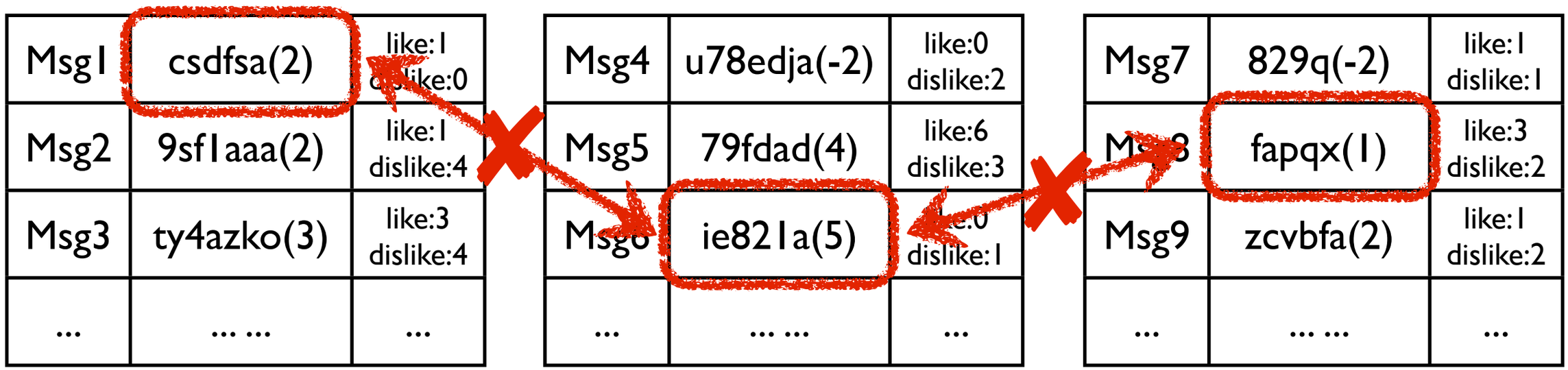
Security-Enhanced AnonRep

- 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



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
Msg8	ie821a(5)	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
Msg8	ie821a(101)	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*

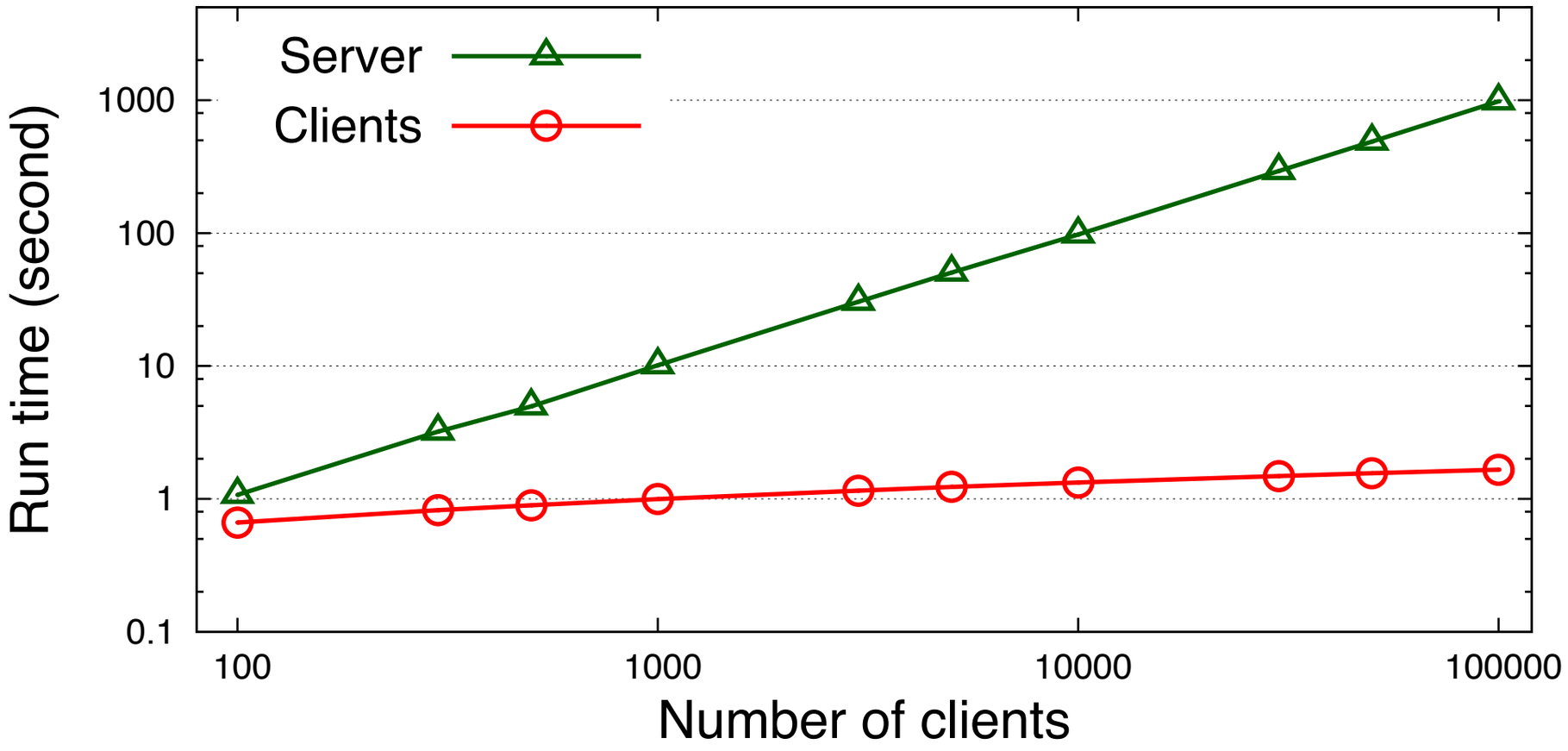
Road-Map

- Motivations
- AnonRep Design
- Practical Considerations
- Evaluation

Implementation

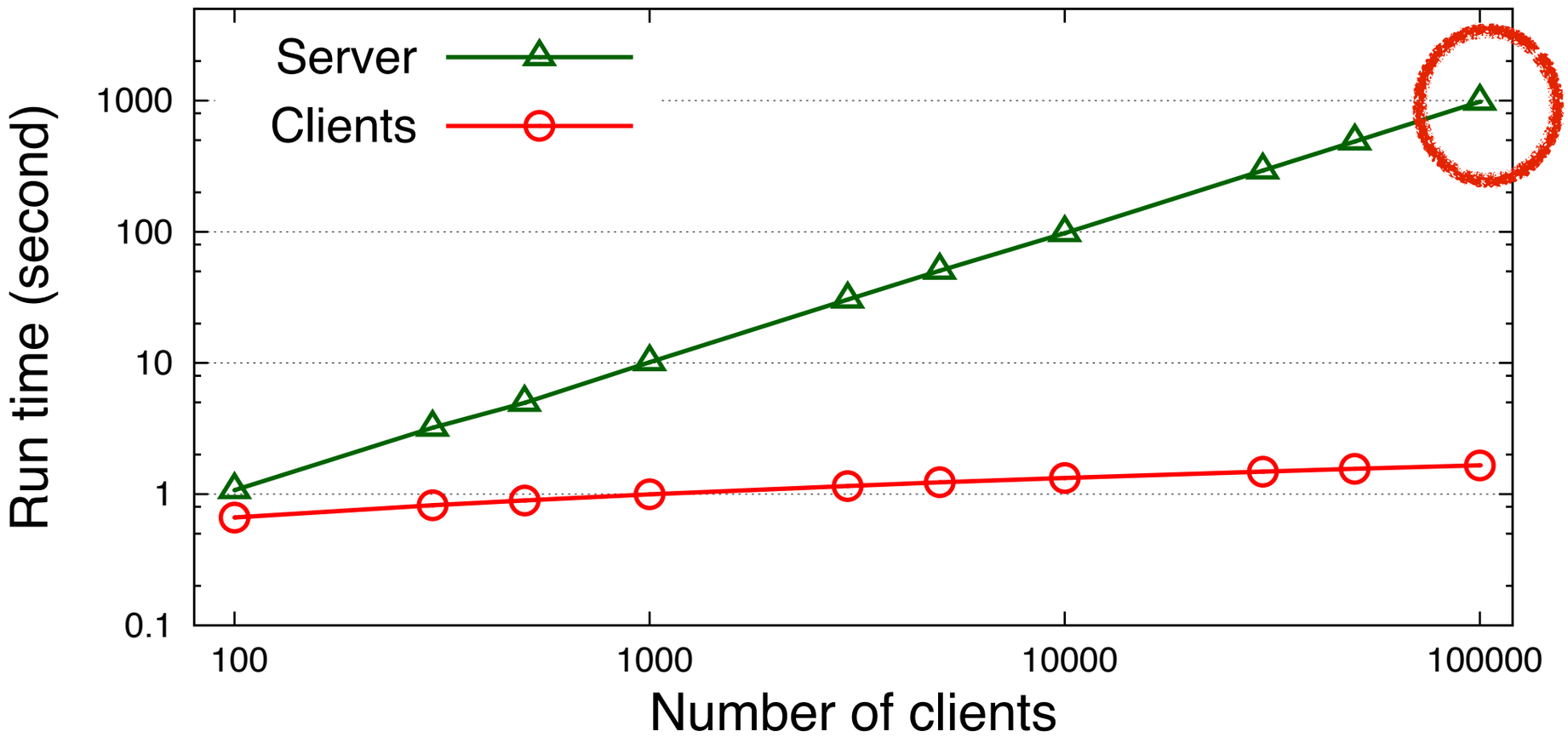
- A working prototype in Go Language
  - Heavily depends on DeDiS Crypto Go library
    https://github.com/DeDiS/crypto
  - Our prototype is open source
    https://github.com/anonyreputation/anonCred

Evaluation



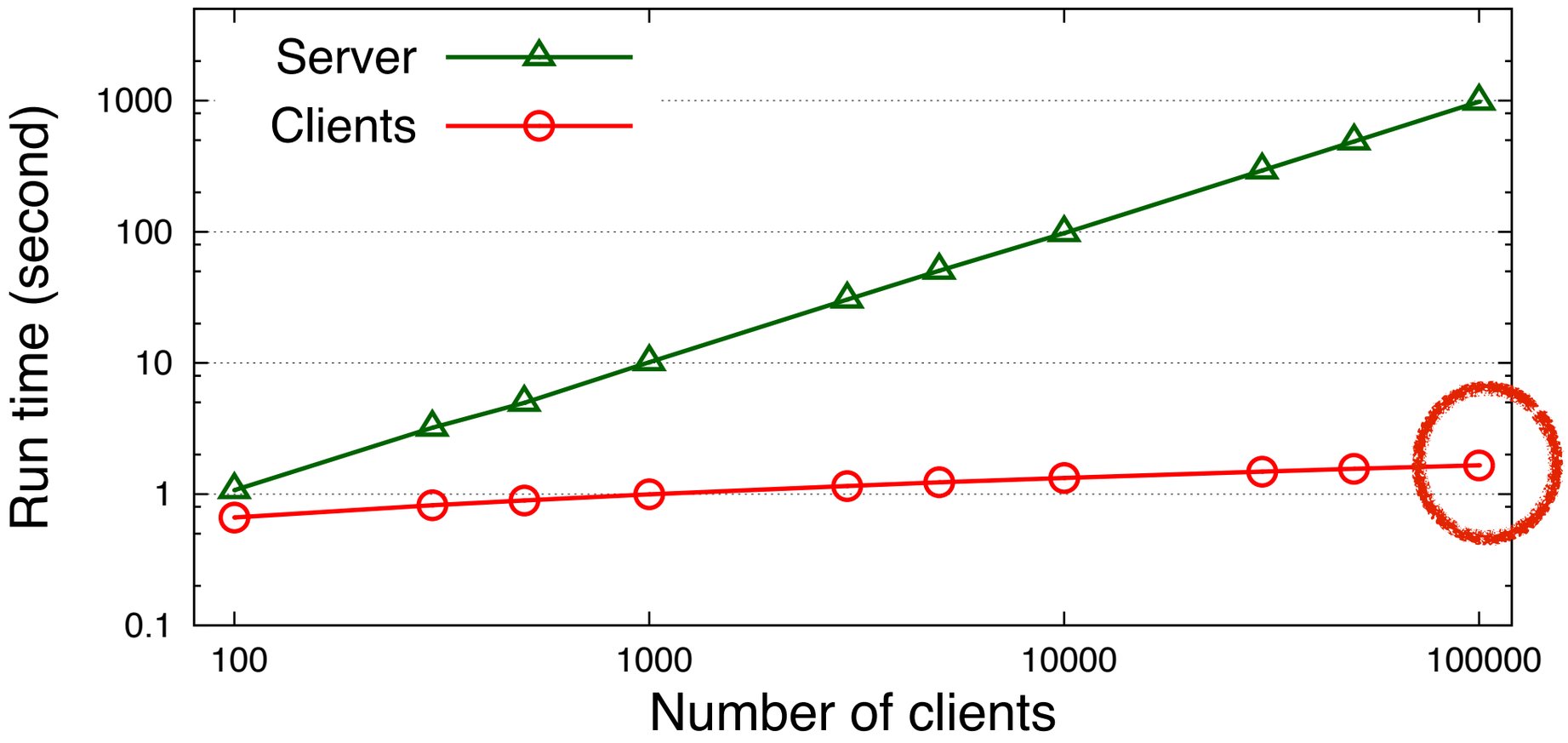
Computational overhead in announcement step

Evaluation



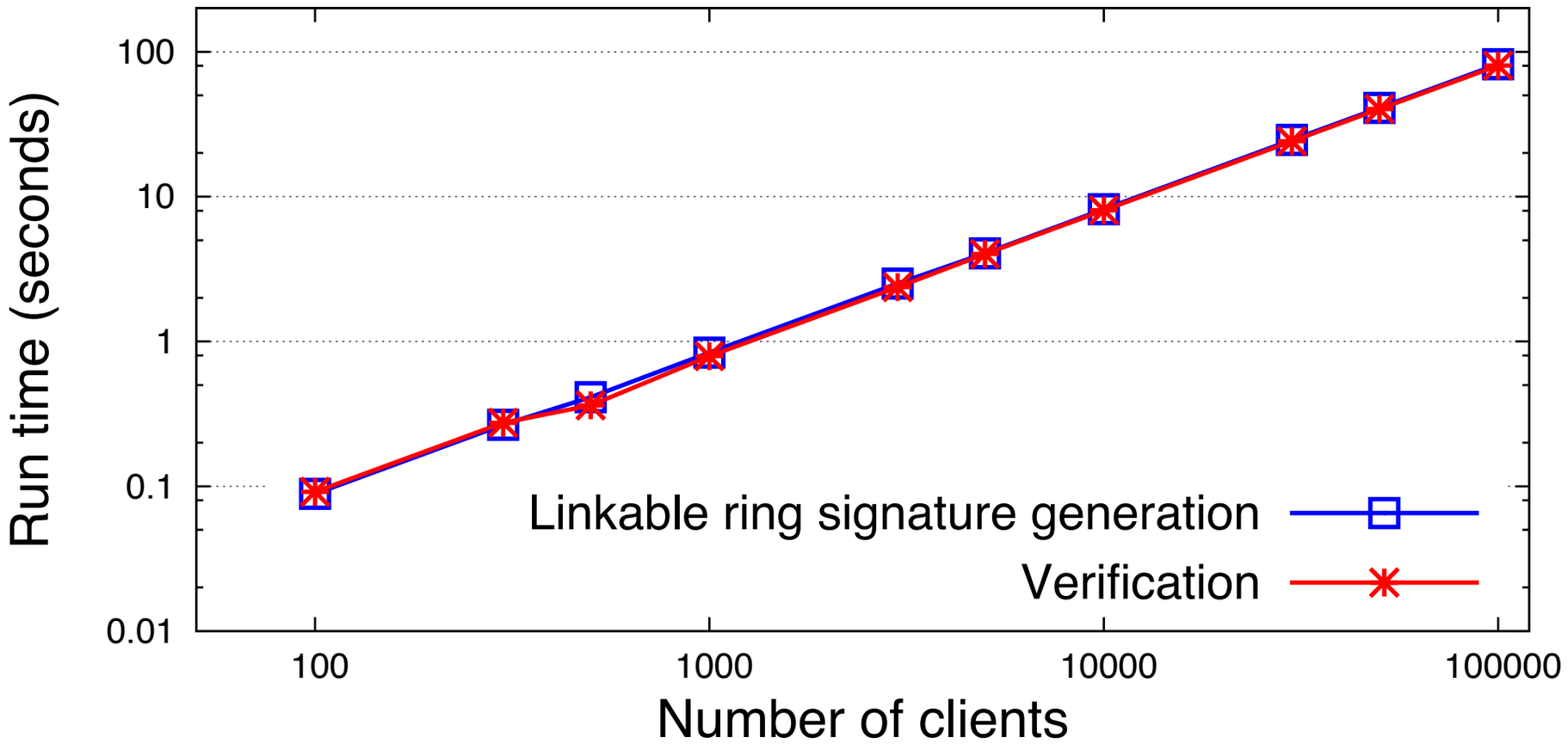
Computational overhead in announcement step

Evaluation



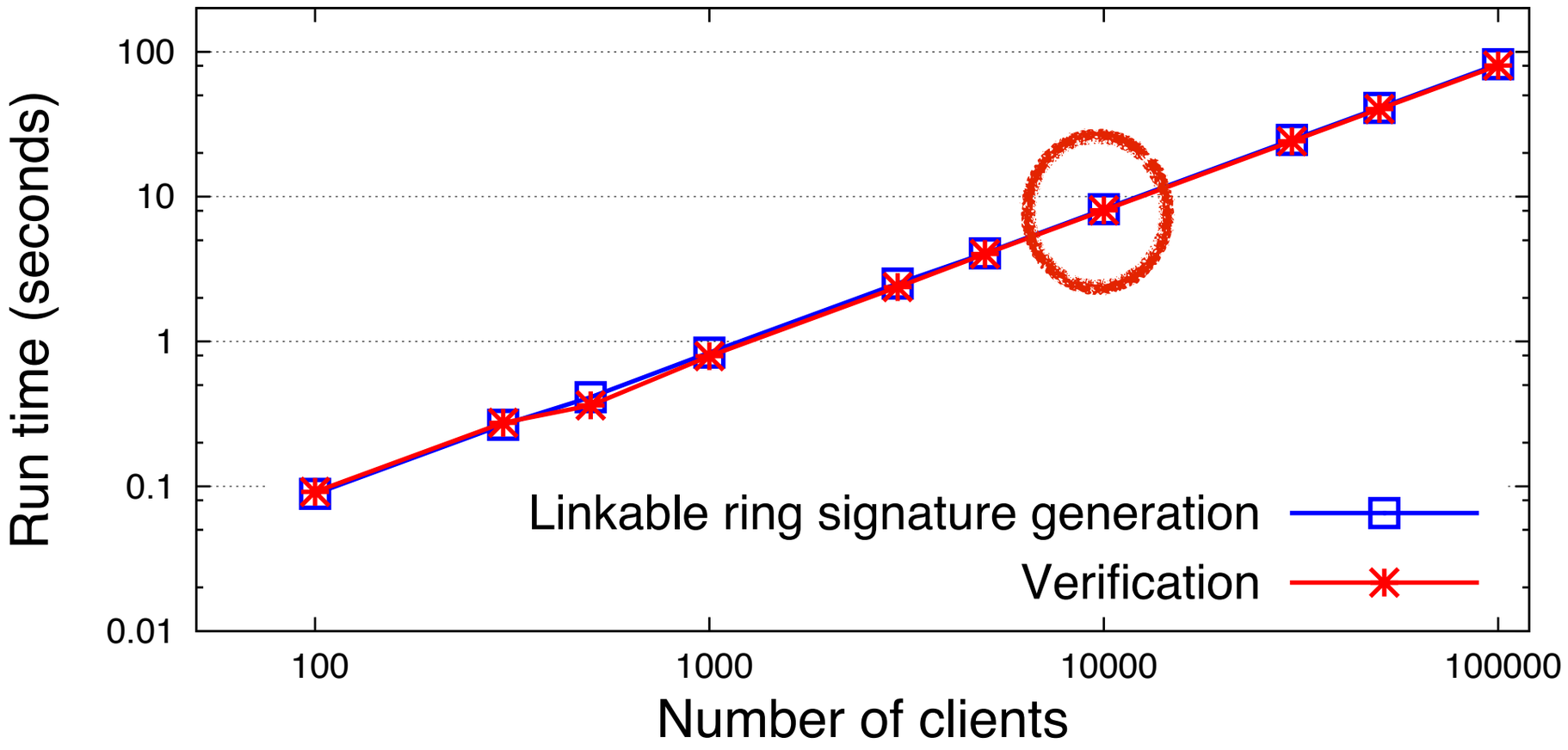
Computational overhead in announcement step

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/