

Finding Safety in Numbers with Secure Allegation Escrows

Venkat Arun^{*}, Aniket Kate⁺, Deepak Garg[^], Peter
Druschel[^] and Bobby Bhattacharjee[#]

^{*}MIT ⁺Purdue University

[^]MPI-SWS [#]University of Maryland

Many crimes are underreported
E.g. sexual assault and corruption

Many crimes are underreported
E.g. sexual assault and corruption

Reasons

- Reporting can be isolating or retraumatizing
- Fear of professional/personal harassment by the perpetrator
- Fear of not being believed

Many crimes are underreported
E.g. sexual assault and corruption

Reasons

- Reporting can be isolating or retraumatizing
- Fear of professional/personal harassment by the perpetrator
- Fear of not being believed

It is easier to report with corroborators

We can build safety in numbers

Many crimes are underreported
E.g. sexual assault and corruption

Reasons

- Reporting can be isolating or retraumatizing
- Fear of professional/personal harassment by the perpetrator
- Fear of not being believed

It is easier to report with corroborators

We can build safety in numbers

90% of sexual assaults are committed by repeat perpetrators

Many crimes are underreported
E.g. sexual assault and corruption

Reasons

- Reporting can be isolating or retraumatizing
- Fear of professional/personal harassment by the perpetrator
- Fear of not being believed

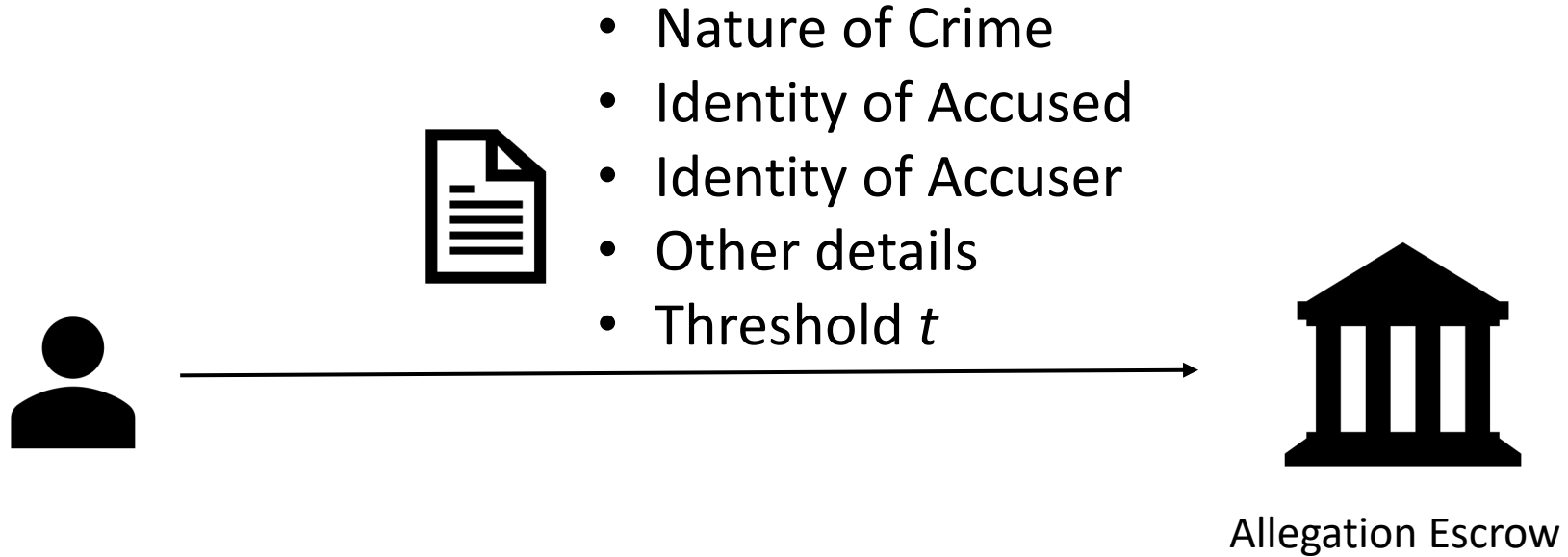
It is easier to report with corroborators

We can build safety in numbers

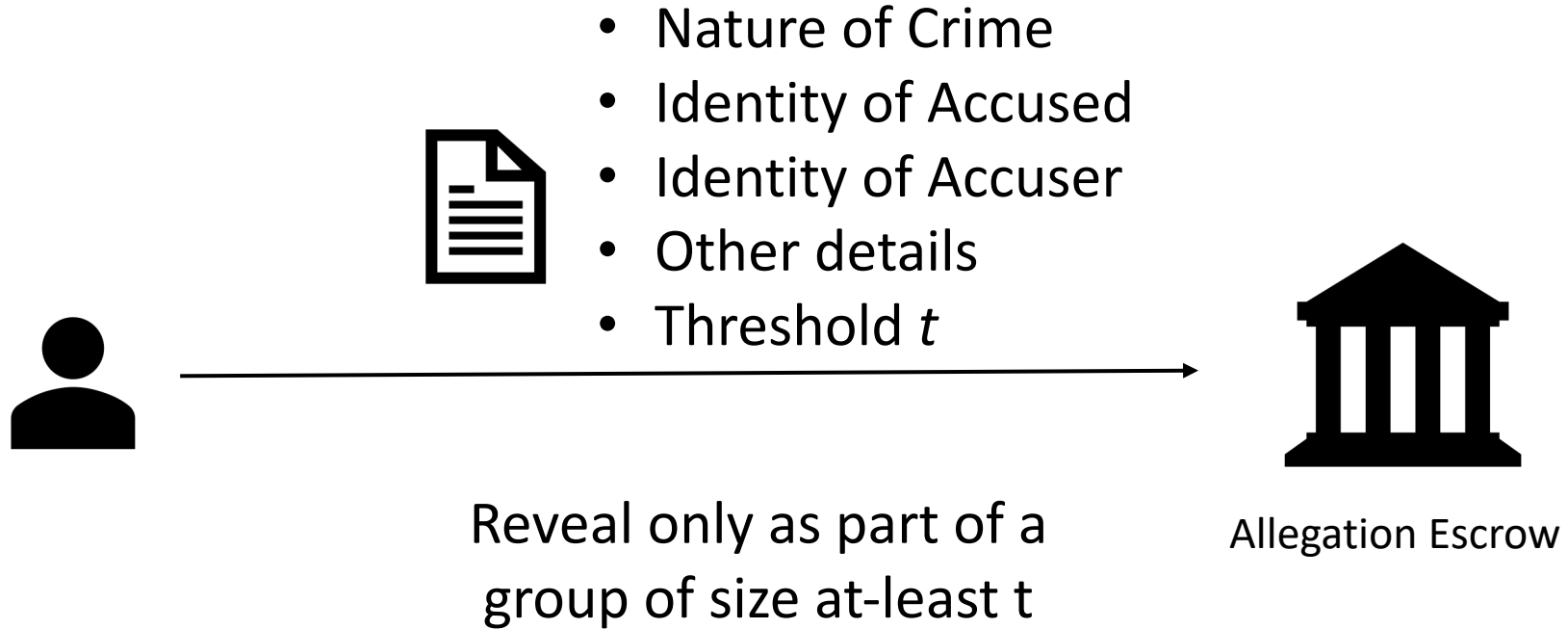
90% of sexual assaults are committed by repeat perpetrators

Many people are aware of corruption

Allegation Escrow: Definition



Allegation Escrow: Definition



Allegation Escrow: Definition

- Nature of Crime
- Identity of Accused

- If allegation is revealed, guaranteed to have corroborators
- A record of the allegation is created early on

Reveal only as part of a
group of size at-least t

Allegation Escrow

Case study: Project Callisto for allegations of sexual assault

- Deployed in 12 college campuses
- 6x more likely to report
- 3x more likely to seek medical and emotional support
- 10-15% records in the system have been matched

Callisto is a single trusted party

Callisto is a single trusted party

- Callisto has all information (as plaintext), and must be trusted to keep it secret

Callisto is a single trusted party

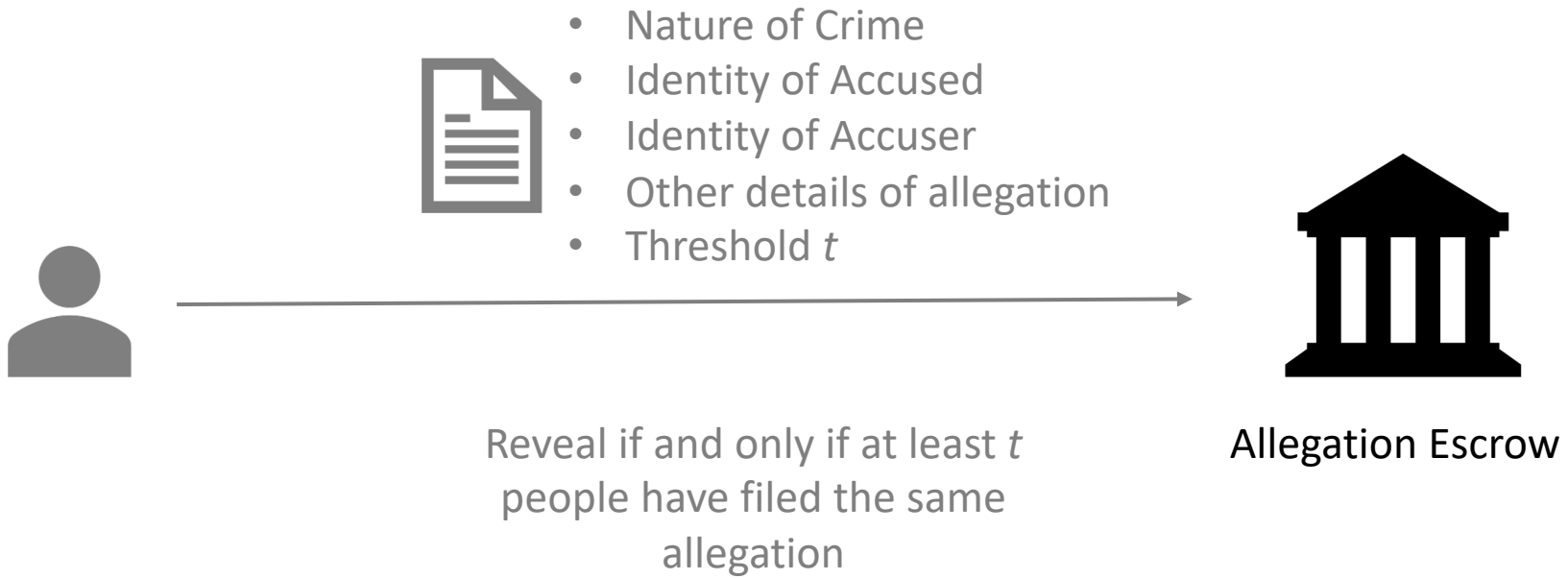
- Callisto has all information (**as plaintext**), and must be trusted to keep it secret
- There are motivated adversaries (who may be influential)

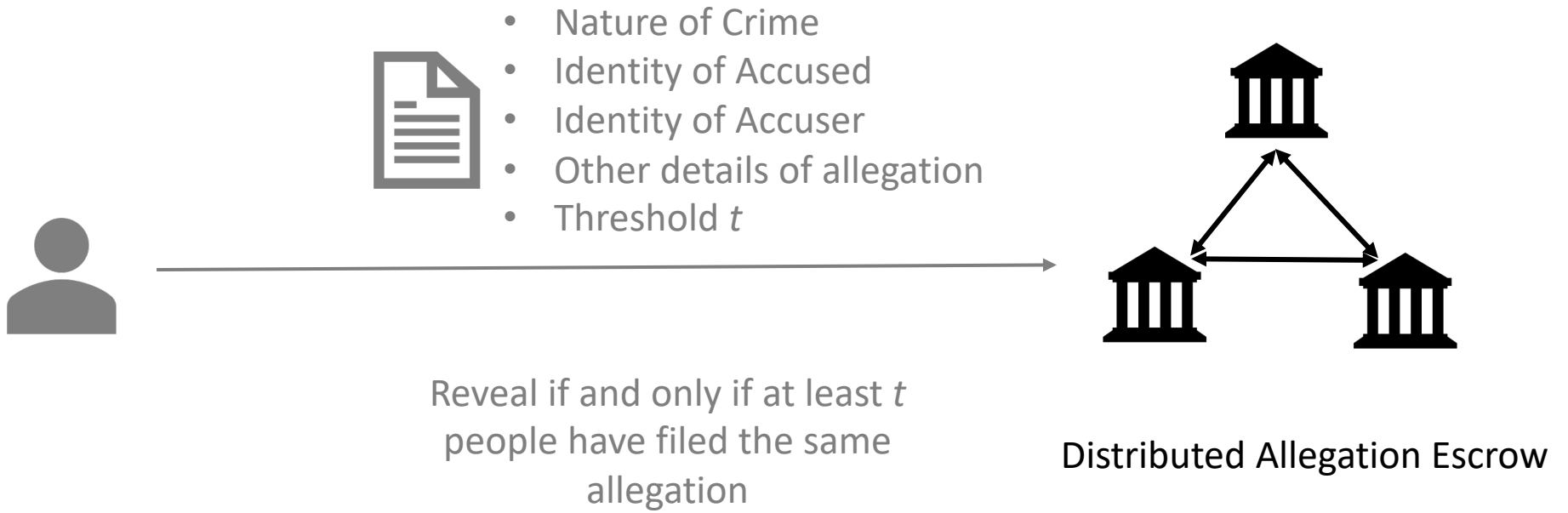
Callisto is a single trusted party

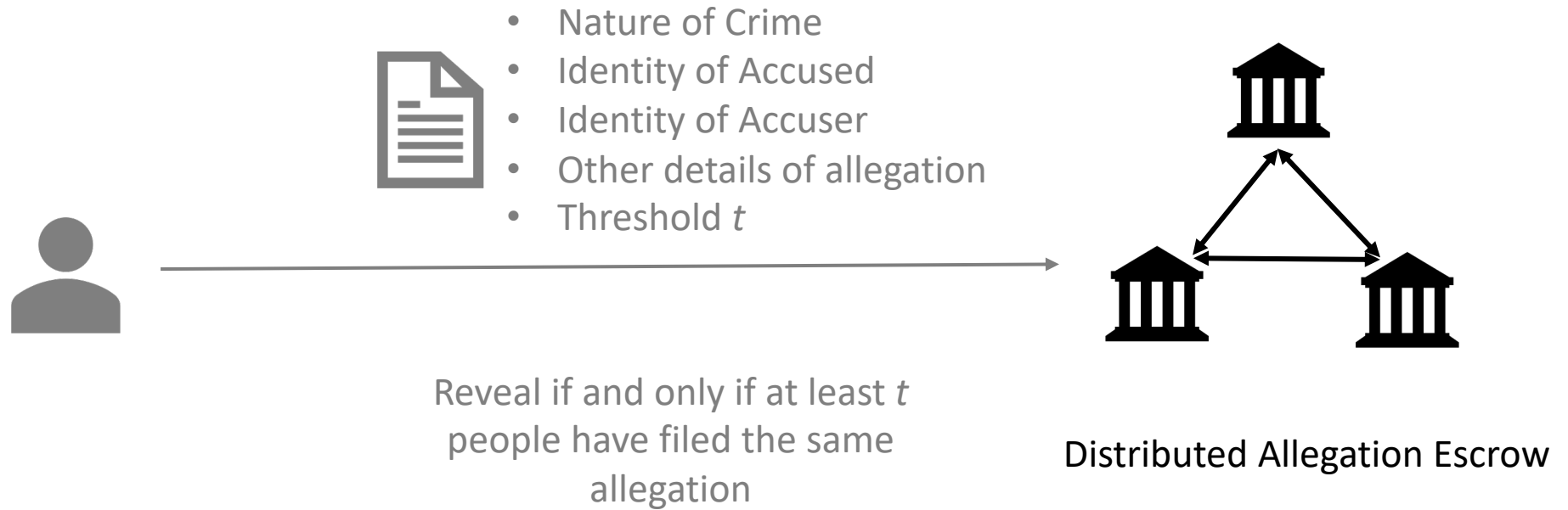
- Callisto has all information (**as plaintext**), and must be trusted to keep it secret
- There are motivated adversaries (who may be influential)
 - Perpetrator may try to suppress allegation or go after the victim

Callisto is a single trusted party

- Callisto has all information (**as plaintext**), and must be trusted to keep it secret
- There are motivated adversaries (who may be influential)
 - Perpetrator may try to suppress allegation or go after the victim
 - Journalists looking for a story







Secrets are safe as long as a majority of these escrows are honest

Who are the escrows?

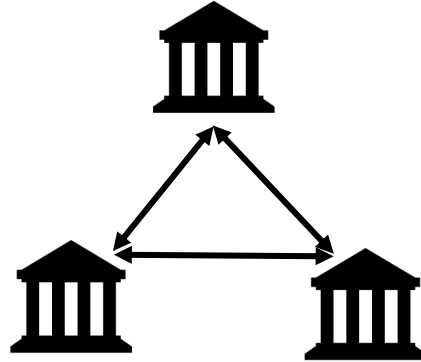


Who are the escrows?



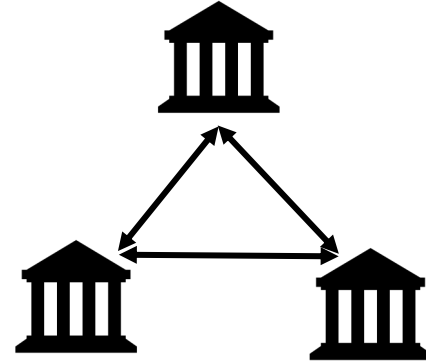
- Non-Profit Organizations
- Educational institutions
- Government entities
- Corporate entities

Who uses the escrows?

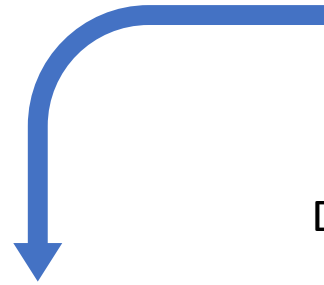


Distributed Allegation Escrow

Who uses the escrows?



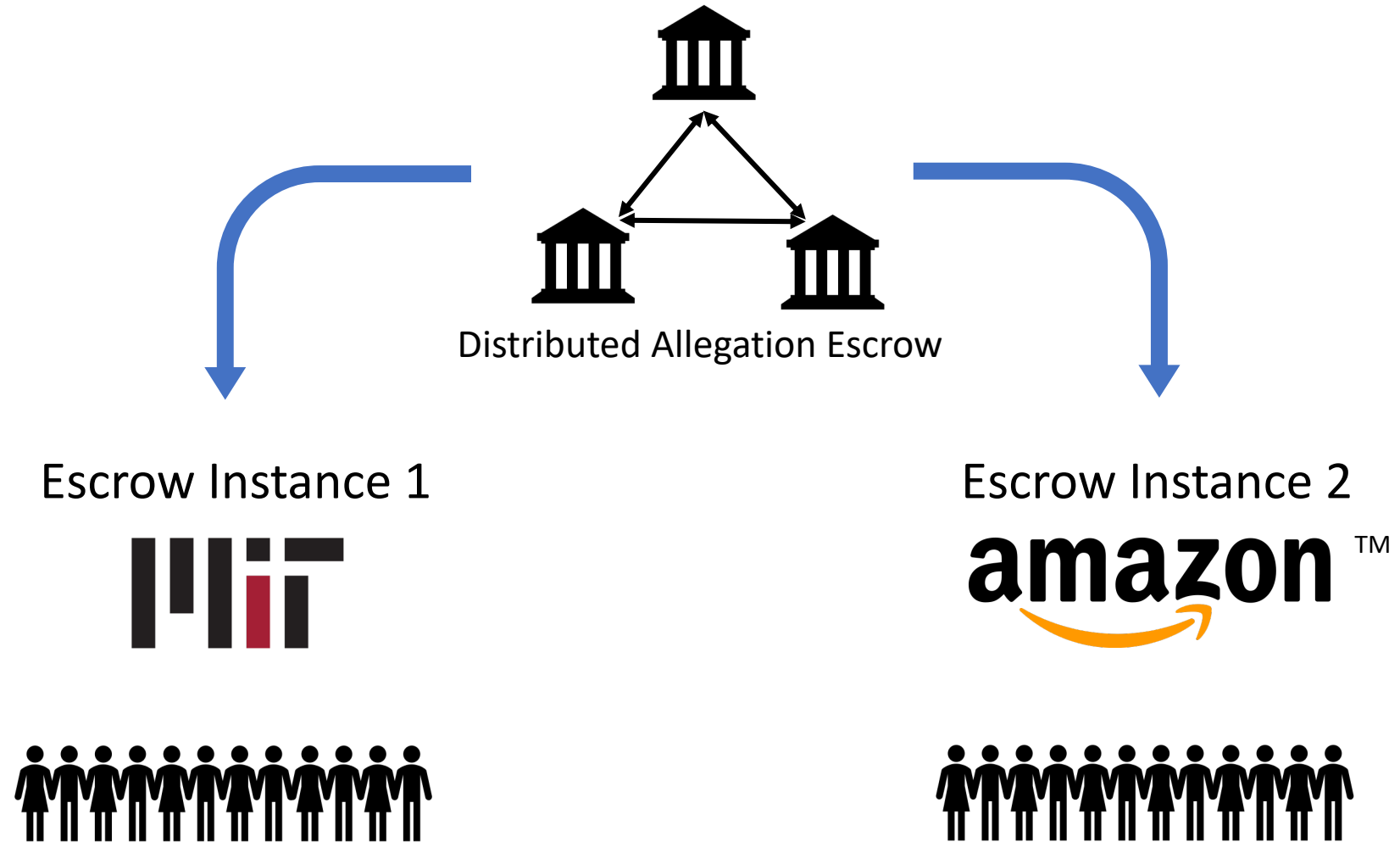
Distributed Allegation Escrow



Escrow Instance 1



Who uses the escrows?



When are allegations revealed?

When are allegations revealed?

Alleger A



When are allegations revealed?

Alleger A



Accusing

“Bob”

When are allegations revealed?

Alleger A





Accusing

“Bob”

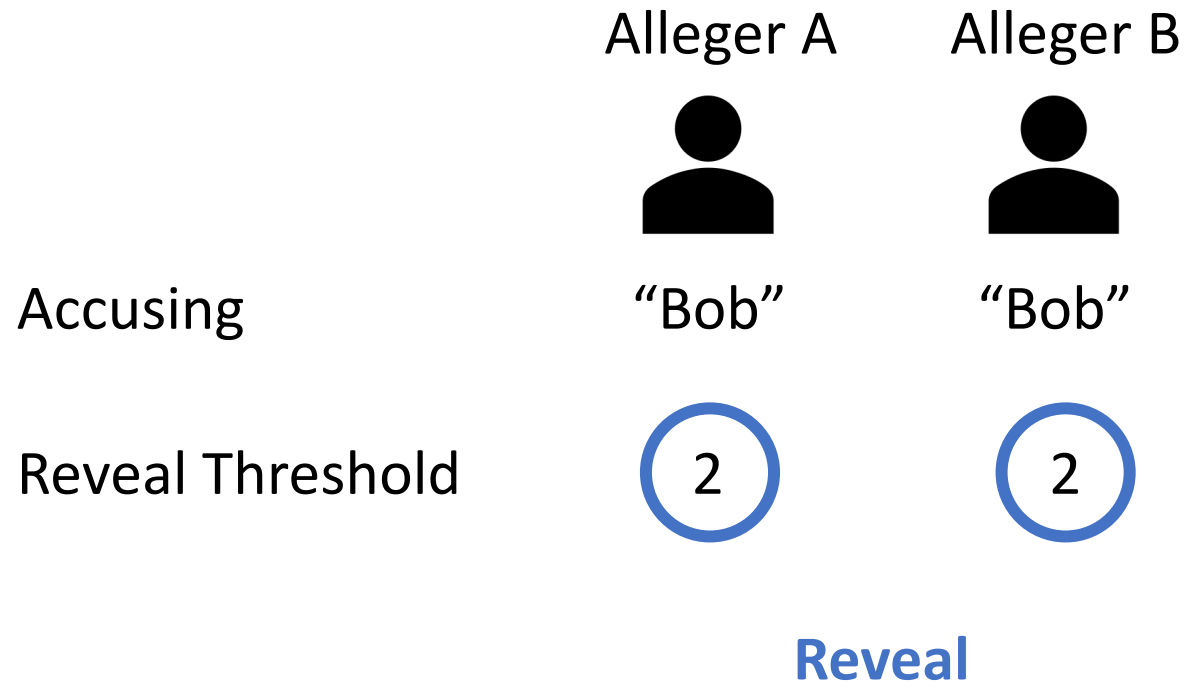
Reveal Threshold

2

When are allegations revealed?

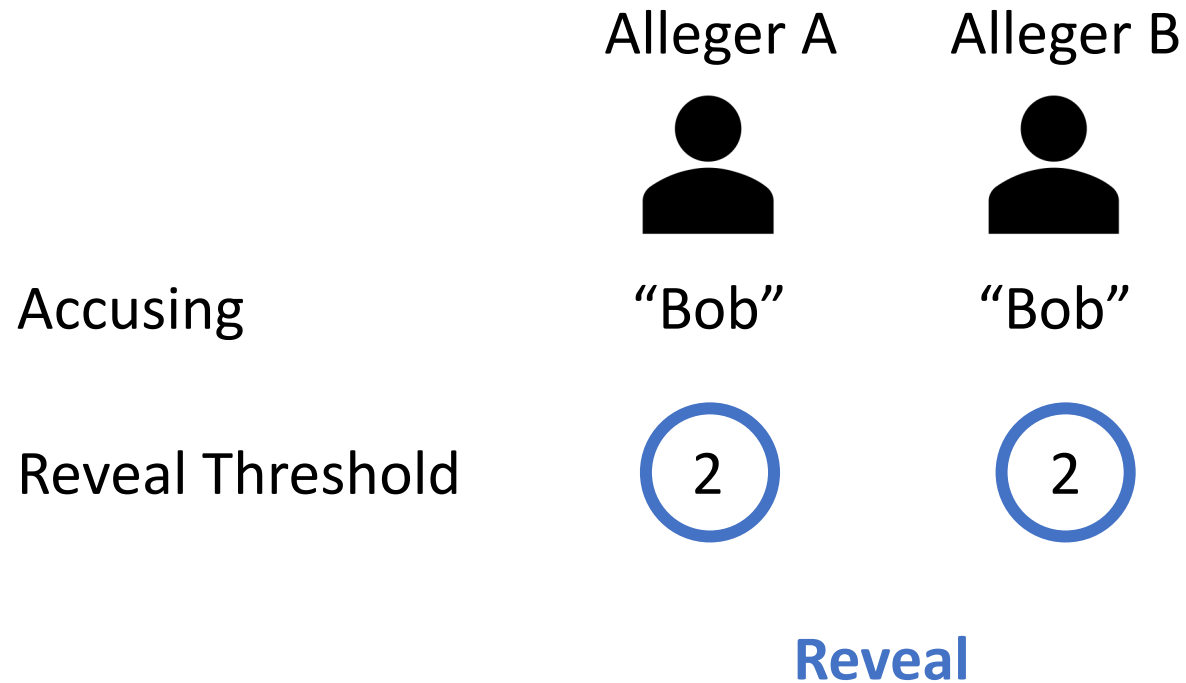
	Alleger A	Alleger B
Accusing	 "Bob"	 "Bob"
Reveal Threshold	2	2

When are allegations revealed?





When are allegations revealed?

We allow each allegor to pick their own reveal threshold



When are allegations revealed?

	Alleger A	Alleger B
Accusing	 "Bob"	 "Bob"
Reveal Threshold	2	3

When are allegations revealed?

A set of allegations S is revealed if and only if all allegations in S have threshold $\leq |S|$

Alleger A



“Bob”

Alleger B



“Bob”

Accusing

Reveal Threshold

2

3

When are allegations revealed?

A set of allegations S is revealed if and only if all allegations in S have threshold $\leq |S|$

Alleger A



“Bob”

Alleger B



“Bob”

Accusing

Reveal Threshold

2

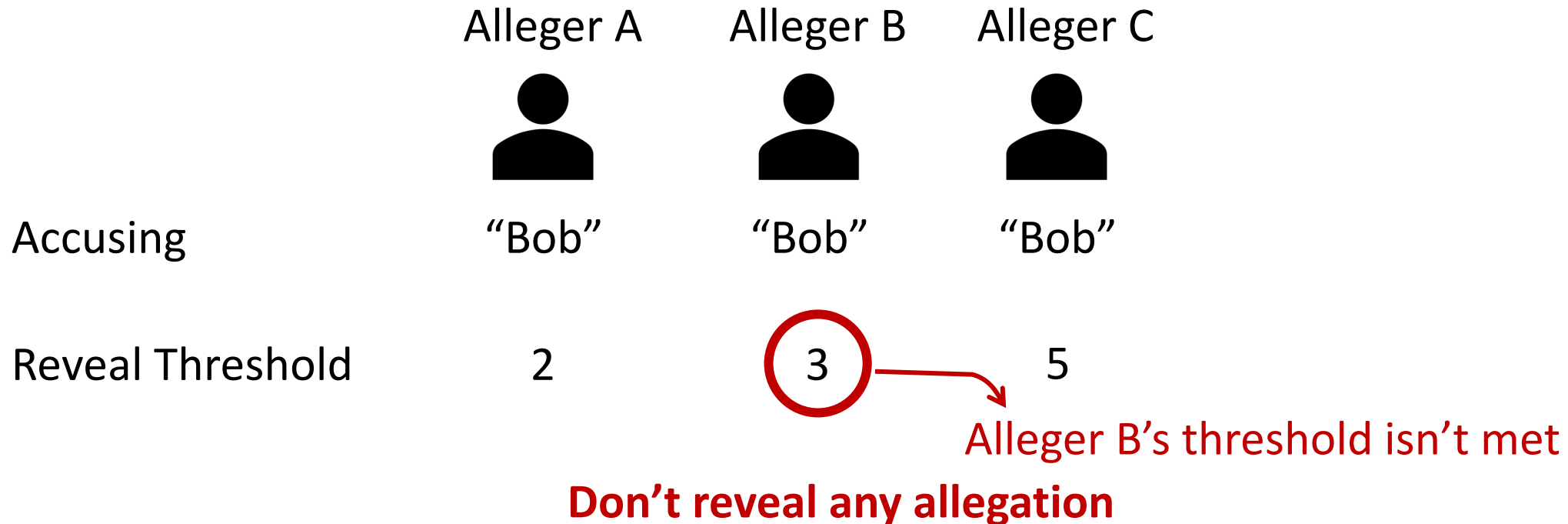
3

Alleger B's threshold isn't met

Don't reveal any allegation

When are allegations revealed?

A set of allegations S is revealed if and only if all allegations in S have threshold $\leq |S|$



When are allegations revealed?

A set of allegations S is revealed if and only if all allegations in S have threshold $\leq |S|$

Alleger A



“Bob”

Alleger B



“Bob”

Alleger C



“Bob”

Accusing

Reveal Threshold

2

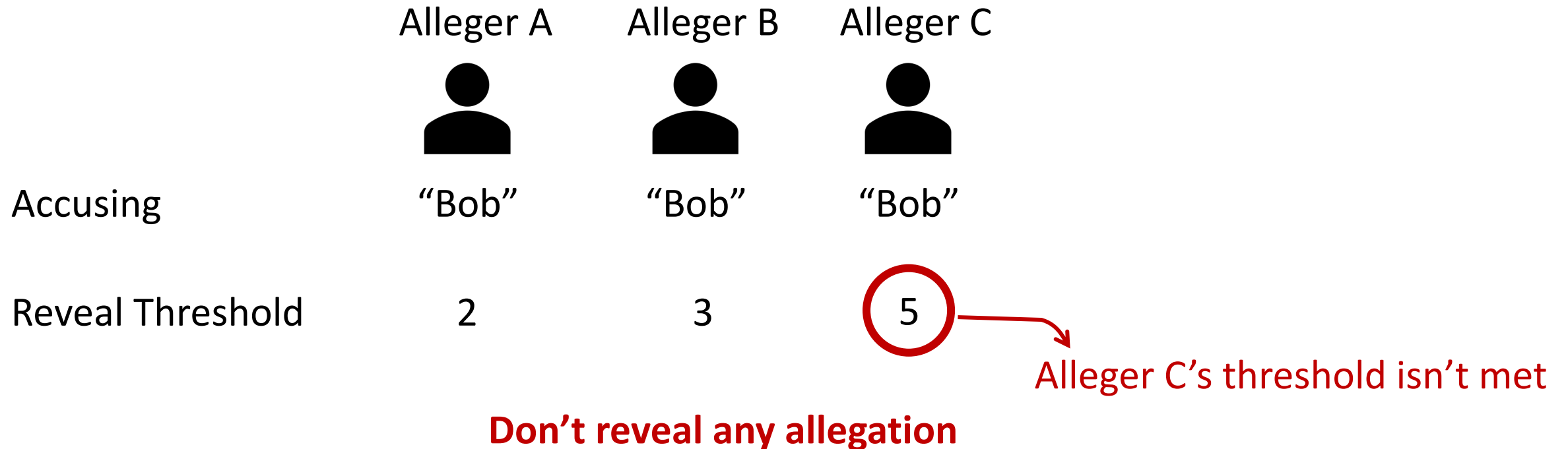
3

5

Don't reveal any allegation





When are allegations revealed?

A set of allegations S is revealed if and only if all allegations in S have threshold $\leq |S|$










When are allegations revealed?

A set of allegations S is revealed if and only if all allegations in S have threshold $\leq |S|$

	Alleger A	Alleger B	Alleger C	Alleger D
				
Accusing	"Bob"	"Bob"	"Bob"	"Bob"
Reveal Threshold	2	3	5	3

When are allegations revealed?

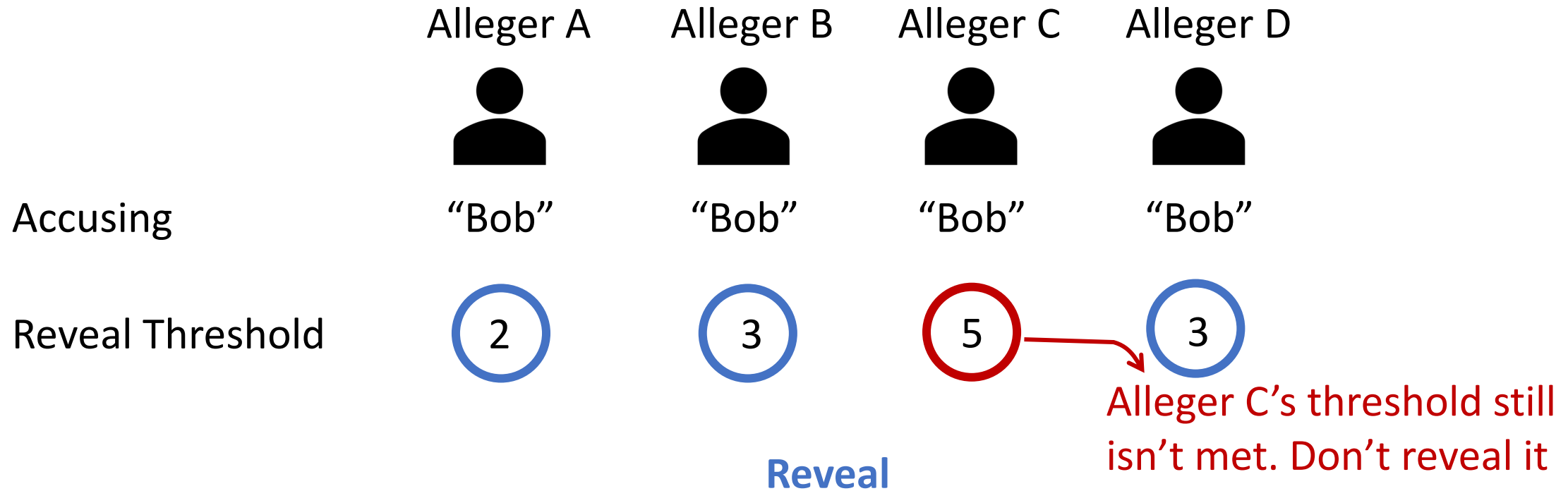
A set of allegations S is revealed if and only if all allegations in S have threshold $\leq |S|$

	Alleger A	Alleger B	Alleger C	Alleger D
Accusing	 "Bob"	 "Bob"	 "Bob"	 "Bob"
Reveal Threshold	 2	 3	5	 3

Reveal

When are allegations revealed?

A set of allegations S is revealed if and only if all allegations in S have threshold $\leq |S|$



When do two allegations 'match'?

When do two allegations 'match'?

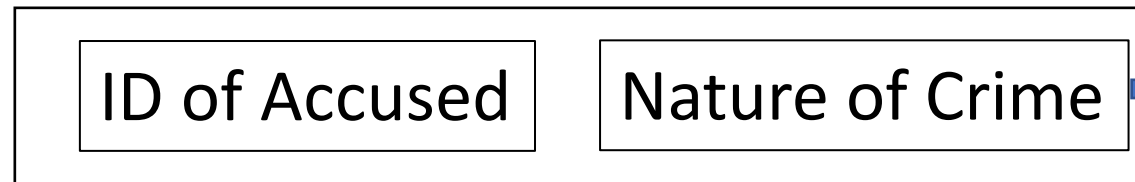
Exact equality on metadata, m

ID of Accused

Nature of Crime

When do two allegations 'match'?

Exact equality on metadata, m



Sexual assault

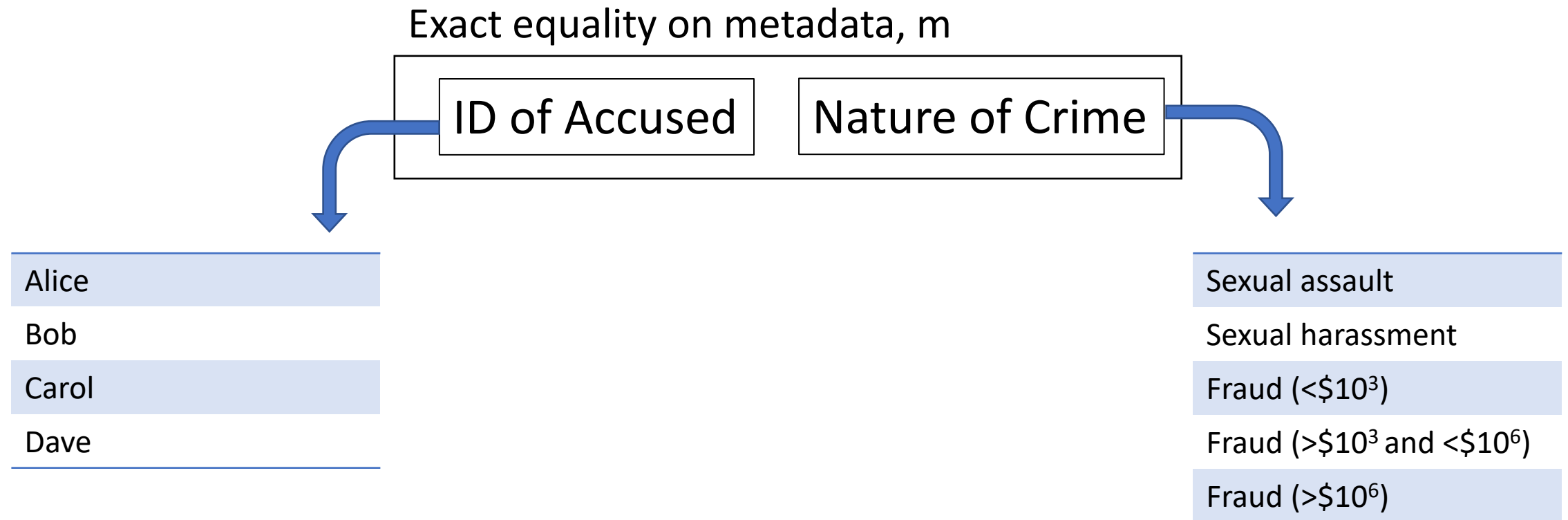
Sexual harassment

Fraud ($< \$10^3$)

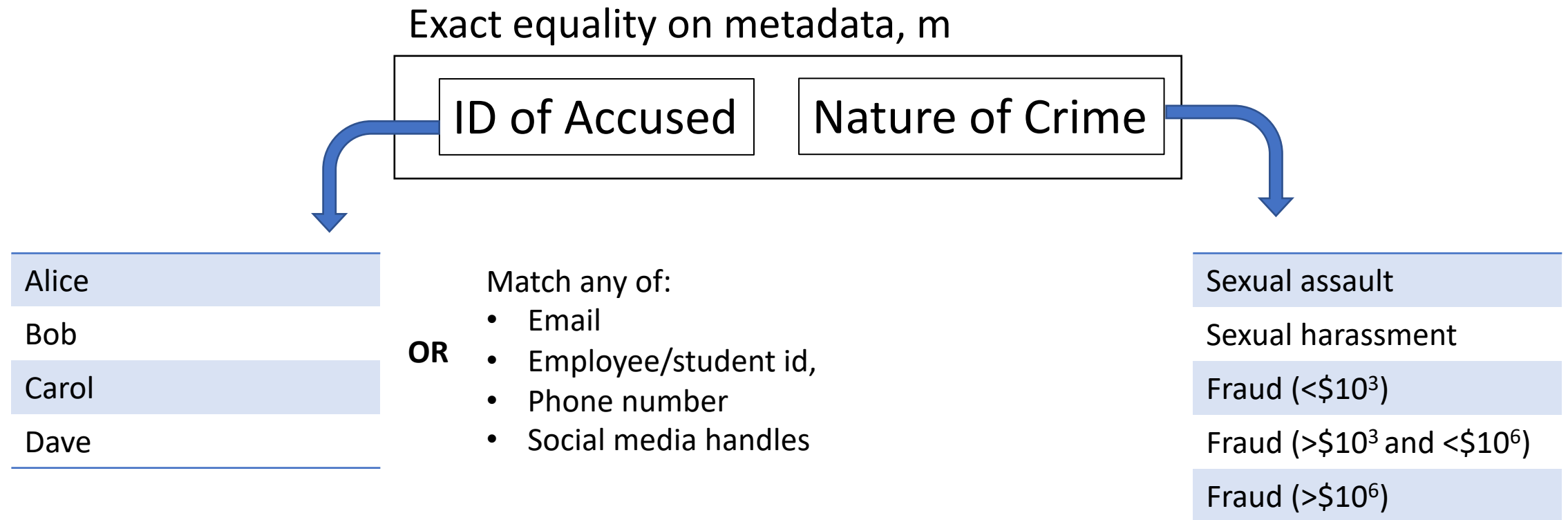
Fraud ($> \$10^3$ and $< \$10^6$)

Fraud ($> \$10^6$)

When do two allegations 'match'?



When do two allegations 'match'?



Related Work in Cryptography

Related Work in Cryptography

- **Cryptography for Project Callisto** [Callisto: A Cryptographic Approach To Detect Serial Predators Of Sexual Misconduct - SIGCAS]

Related Work in Cryptography

- **Cryptography for Project Callisto** [Callisto: A Cryptographic Approach To Detect Serial Predators Of Sexual Misconduct - SIGCAS]
 - Much weaker threat model

Related Work in Cryptography

- **Cryptography for Project Callisto** [Callisto: A Cryptographic Approach To Detect Serial Predators Of Sexual Misconduct - SIGCAS]
 - Much weaker threat model
- **WhoToo** [Cryptography for #MeToo - POPETS]

Related Work in Cryptography

- **Cryptography for Project Callisto** [Callisto: A Cryptographic Approach To Detect Serial Predators Of Sexual Misconduct - SIGCAS]
 - Much weaker threat model
- **WhoToo** [Cryptography for #MeToo - POPETS]
 - Not scalable: Cost to file an allegation is $O(N)$ if there are N pre-existing allegations in the system. For us, it is $O(1)$

Related Work in Cryptography

- **Cryptography for Project Callisto** [Callisto: A Cryptographic Approach To Detect Serial Predators Of Sexual Misconduct - SIGCAS]
 - Much weaker threat model
- **WhoToo** [Cryptography for #MeToo - POPETS]
 - Not scalable: Cost to file an allegation is $O(N)$ if there are N pre-existing allegations in the system. For us, it is $O(1)$
 - Forces a global reveal threshold. We allow allegers to choose their own thresholds

Scalability is Important

Scalability is Important

- Generic MPC and WhoToo provide $O(N)$ cost per allegation, N – number of allegations already in the system

Scalability is Important

- Generic MPC and WhoToo provide $O(N)$ cost per allegation, N – number of allegations already in the system
 - Susceptible to crippling DoS attacks

Scalability is Important

- Generic MPC and WhoToo provide $O(N)$ cost per allegation, N – number of allegations already in the system
 - Susceptible to crippling DoS attacks
 - We are $O(1)$ and guarantee ‘Bounded MPC’

Scalability is Important

- Generic MPC and WhoToo provide $O(N)$ cost per allegation, N – number of allegations already in the system
 - Susceptible to crippling DoS attacks
 - We are $O(1)$ and guarantee ‘Bounded MPC’
- Larger allegation pool

Scalability is Important

- Generic MPC and WhoToo provide $O(N)$ cost per allegation, N – number of allegations already in the system
 - Susceptible to crippling DoS attacks
 - We are $O(1)$ and guarantee ‘Bounded MPC’
- Larger allegation pool
- Cover traffic to hide timing side channel

Real Identities are Important

Reveal my allegation only if
at-least 3 other people have
filed the same allegation



Alice

Real Identities are Important



Alice

Reveal my allegation only if
at-least 3 other people have
filed the same allegation

Corroborators



Bob

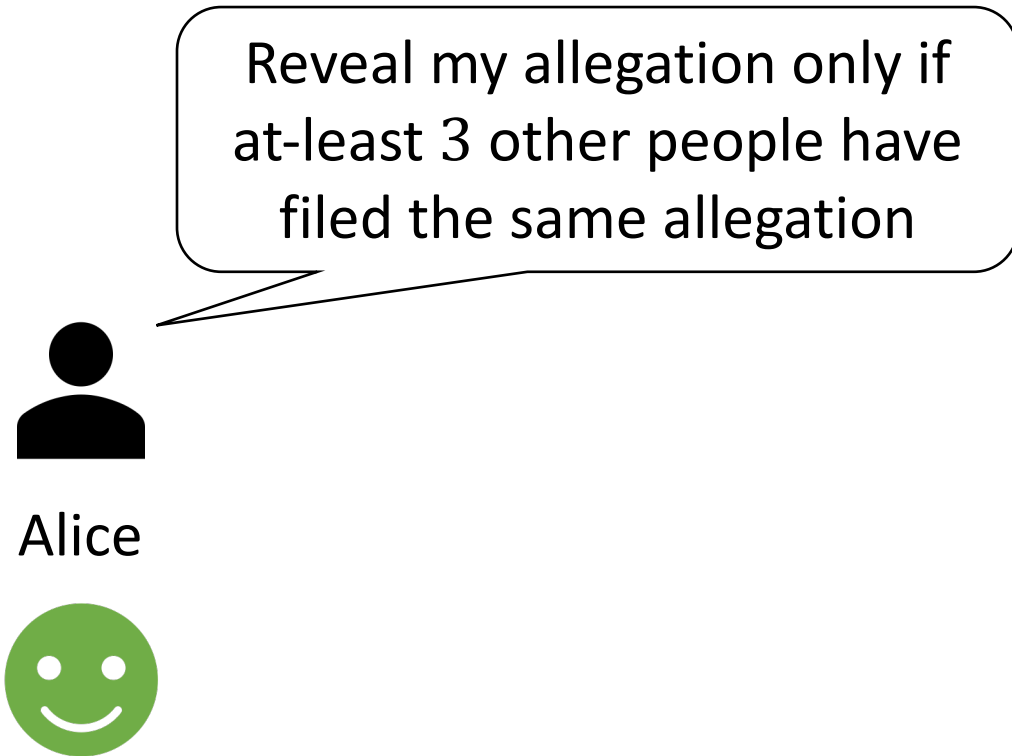


Carol



Dave

Real Identities are Important



Corroborators



Bob

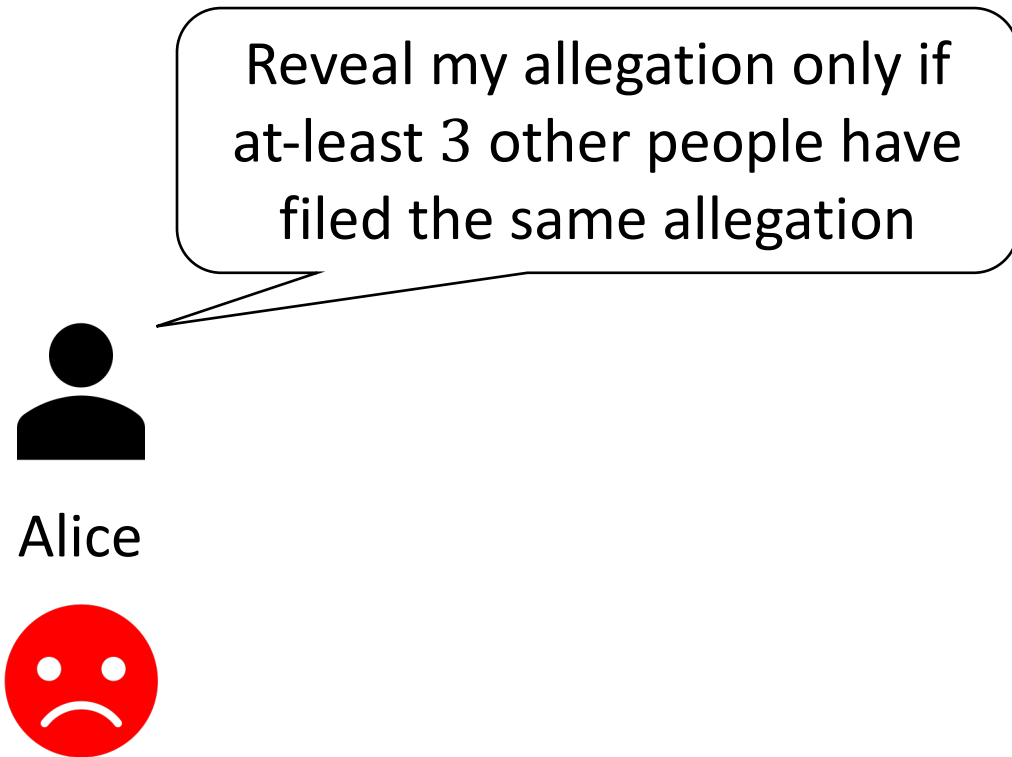


Carol

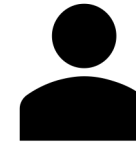


Dave

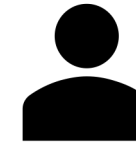
Real Identities are Important



Corroborators



Anonymous Identity 1



Anonymous Identity 2



Anonymous Identity 3

Real Identities are Important



Alice



Reveal my allegation only if at-least 3 other people have filed the same allegation

Could be filed by an adversary to reveal Alice's allegation. Since allegations are anonymous, they face no consequences.

Corroborators



Anonymous Identity 1

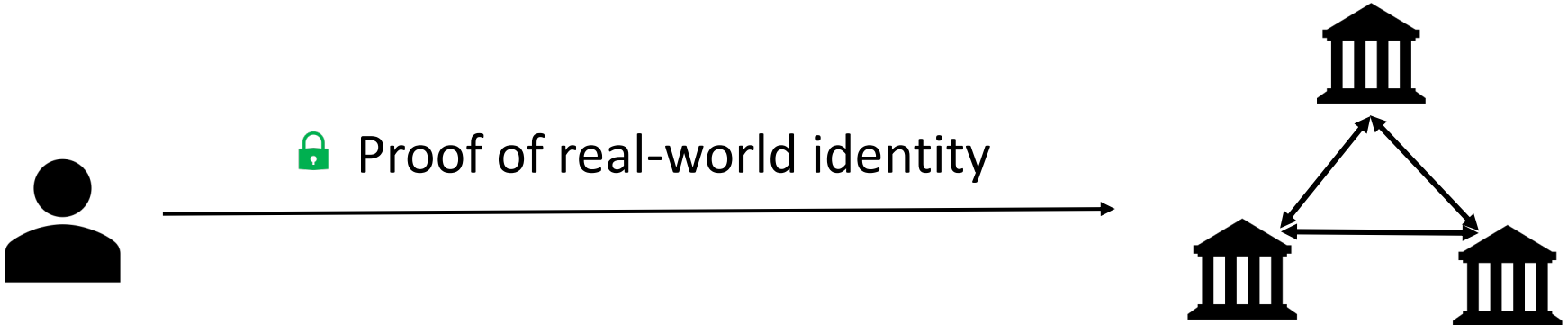


Anonymous Identity 2



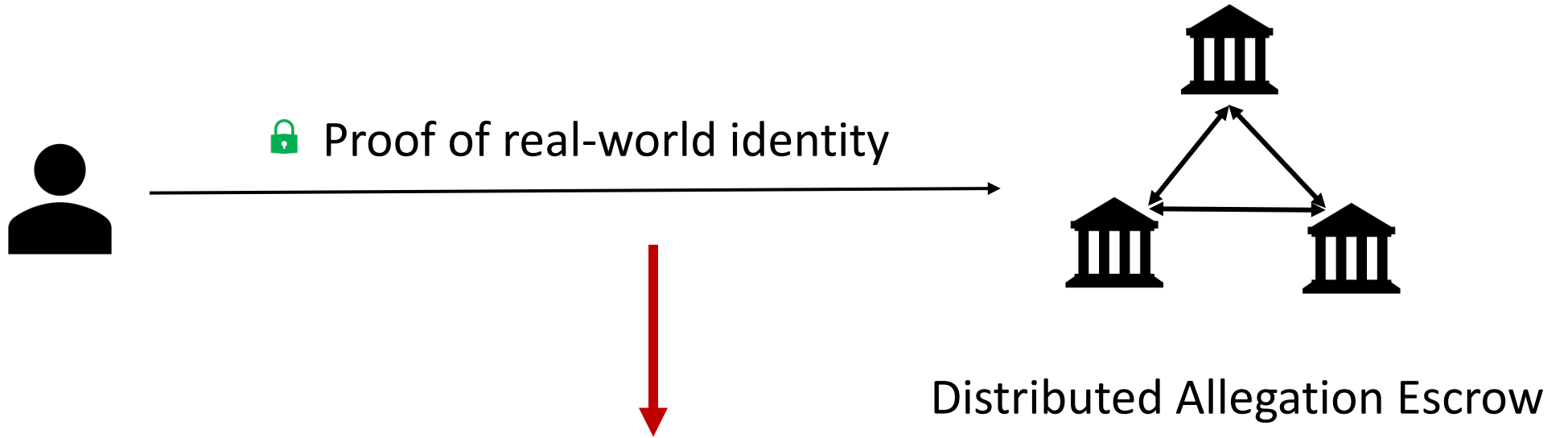
Anonymous Identity 3

Authentication



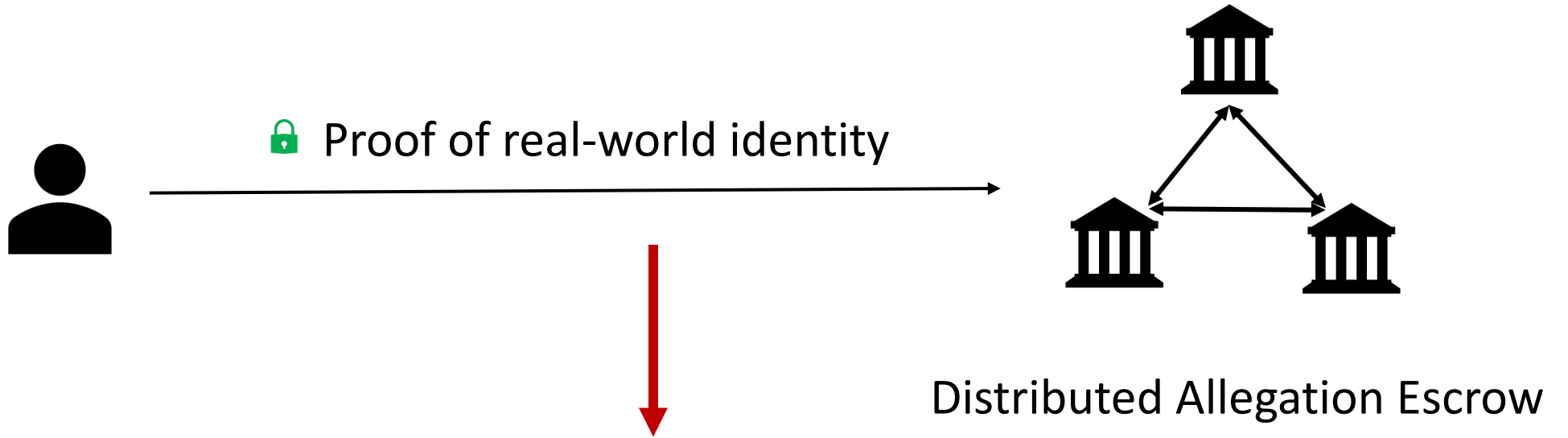
Distributed Allegation Escrow

Authentication



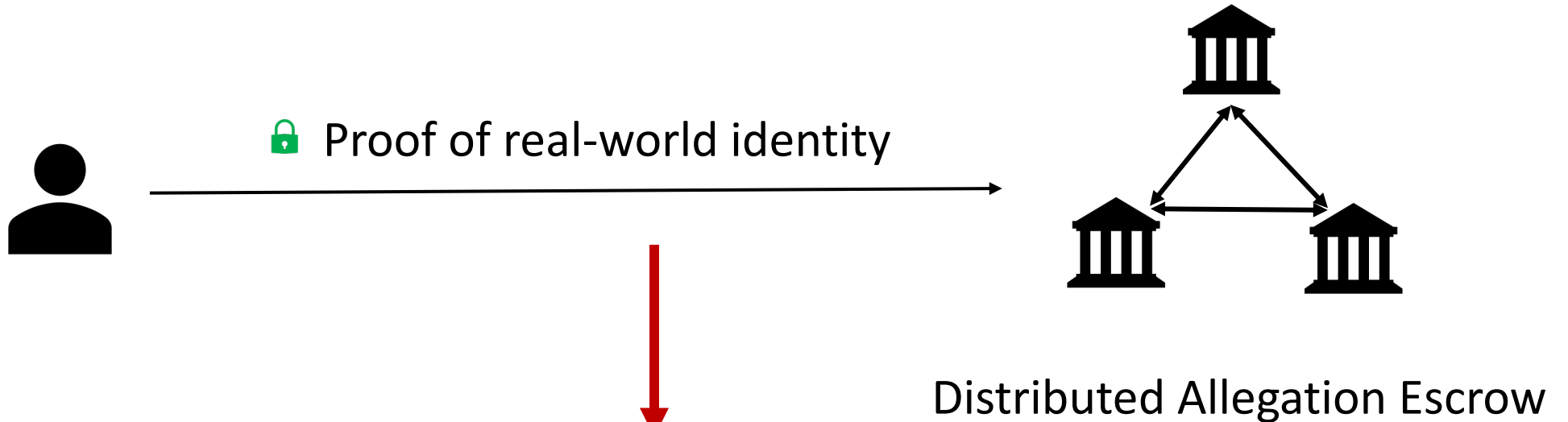
- Shouldn't reveal identity to minority of escrows

Authentication



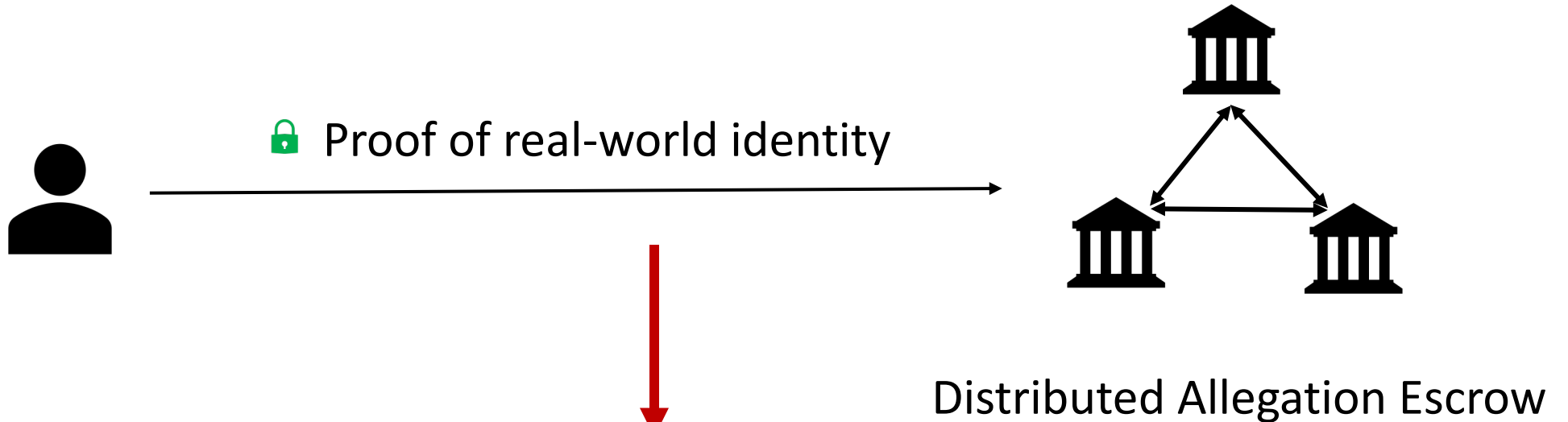
- Shouldn't reveal identity to minority of escrows
- Majority of escrows can determine real identity

Authentication



- Shouldn't reveal identity to minority of escrows
- Majority of escrows can determine real identity
- Identity is revealed when threshold is met

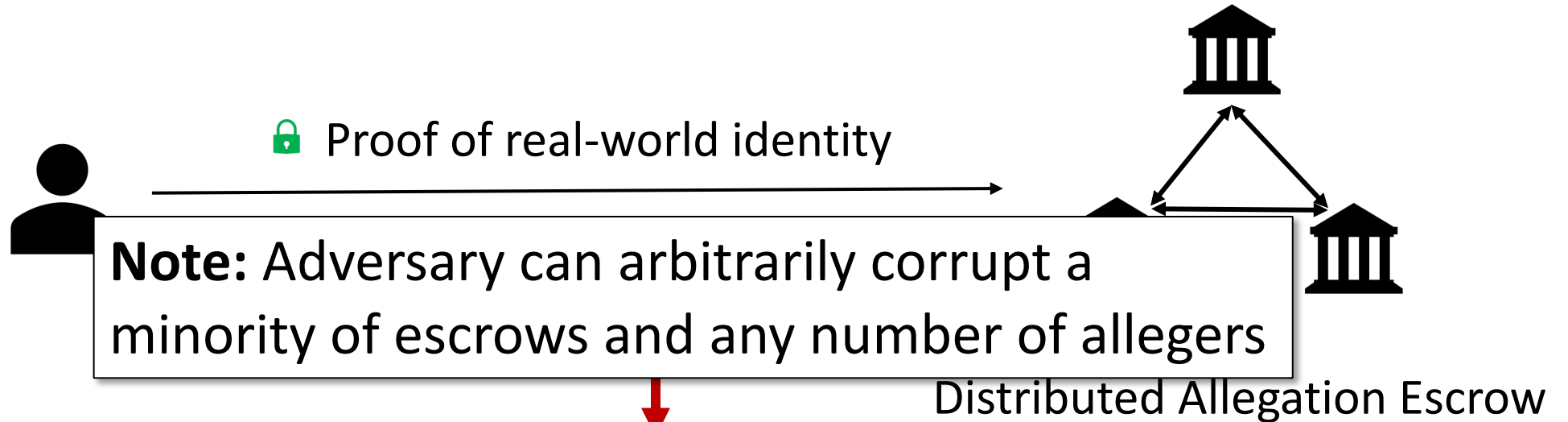
Authentication



- Shouldn't reveal identity to minority of escrows
- Majority of escrows can determine real identity

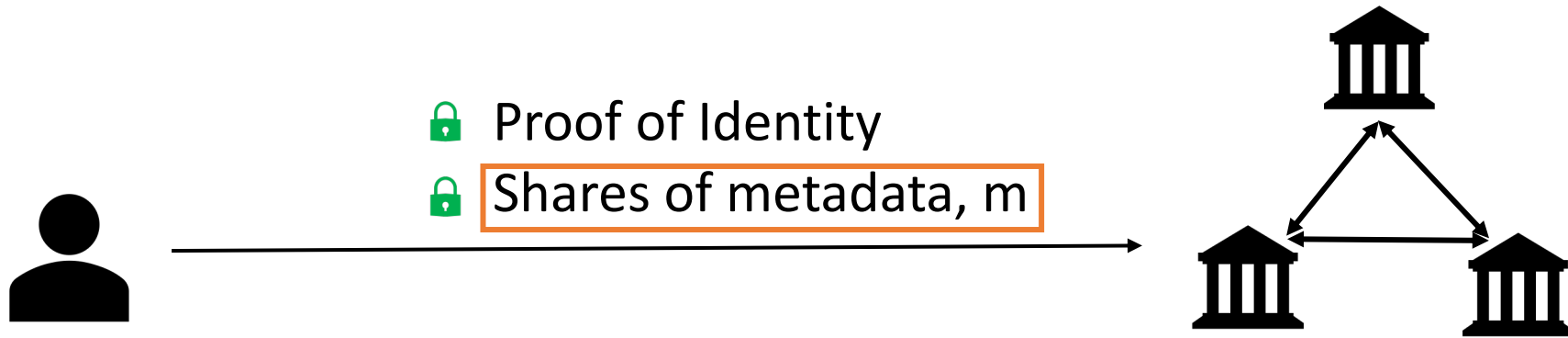
- Identity is revealed when threshold is met
- Remains hidden until then

Authentication

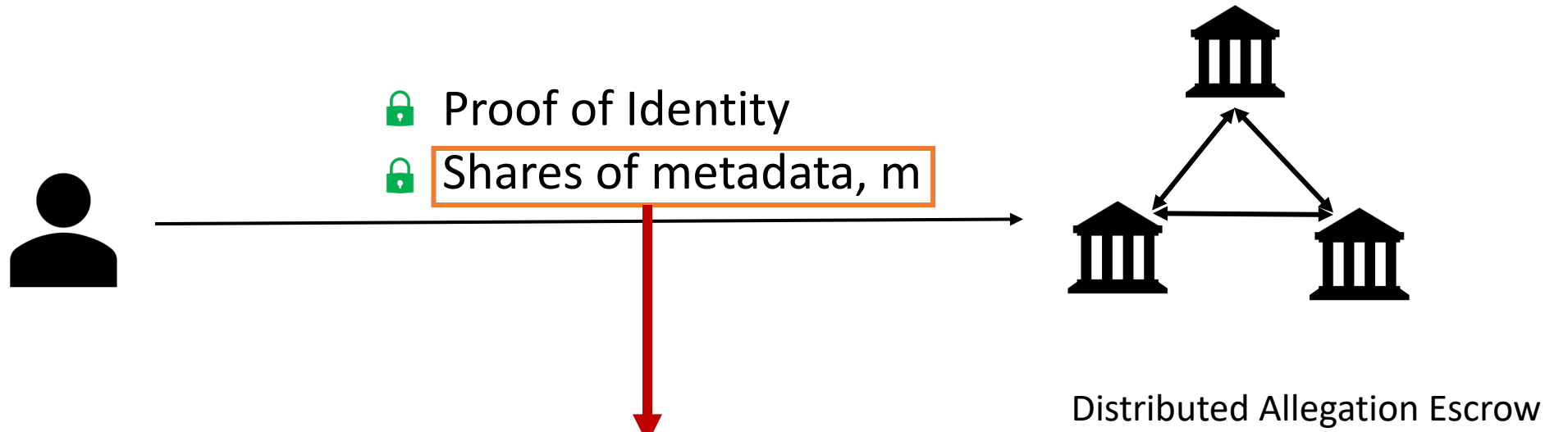


- Shouldn't reveal identity to minority of escrows
- Majority of escrows can determine real identity

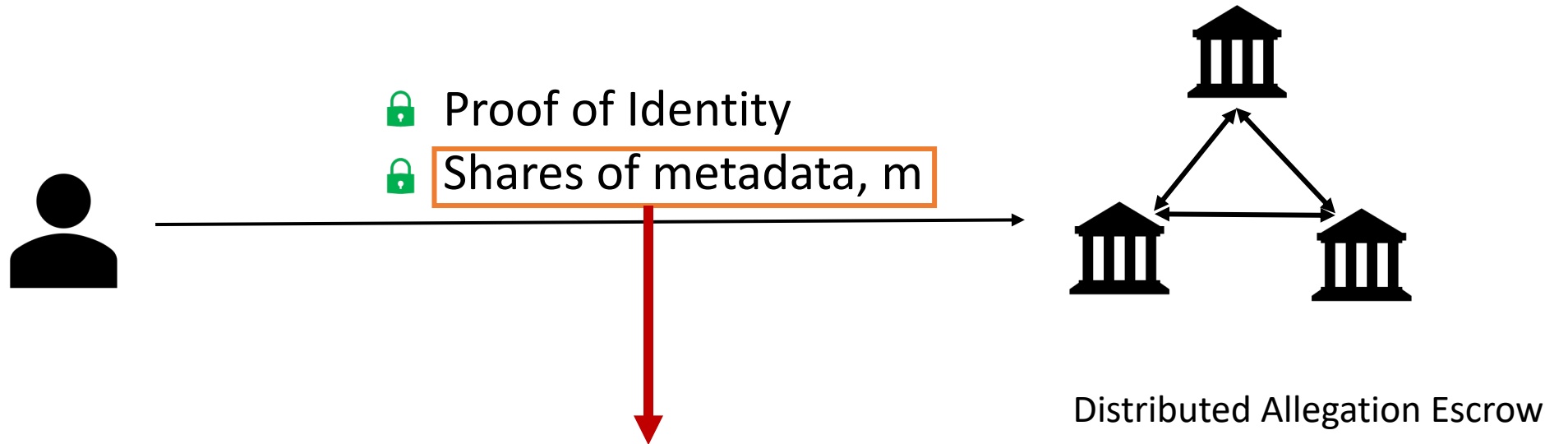
- Identity is revealed when threshold is met
- Remains hidden until then



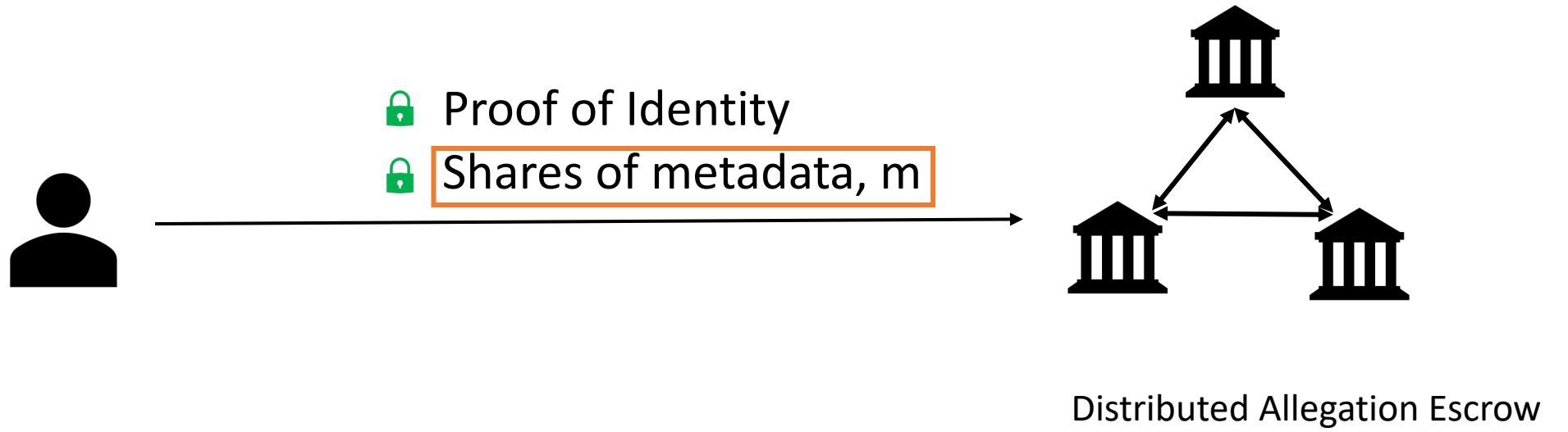
Distributed Allegation Escrow

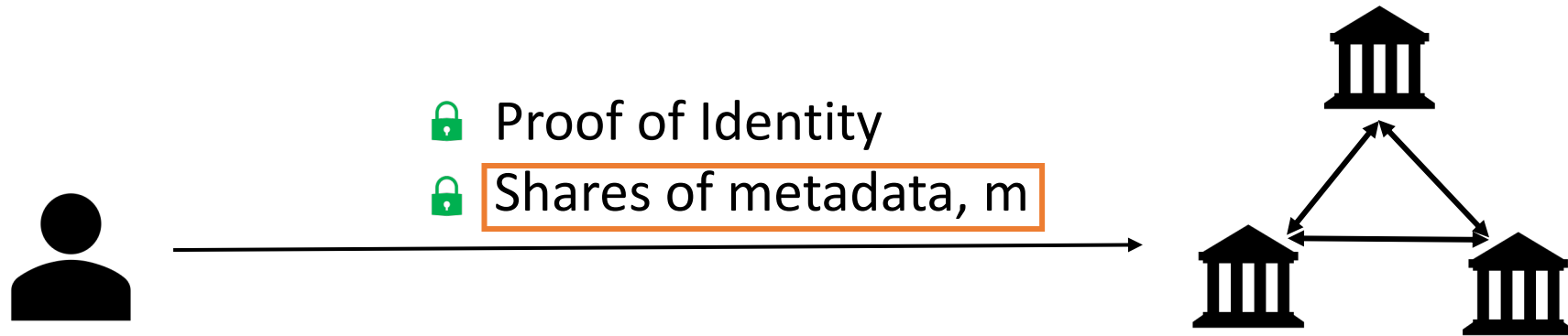


- A majority of escrows must cooperate to reveal m



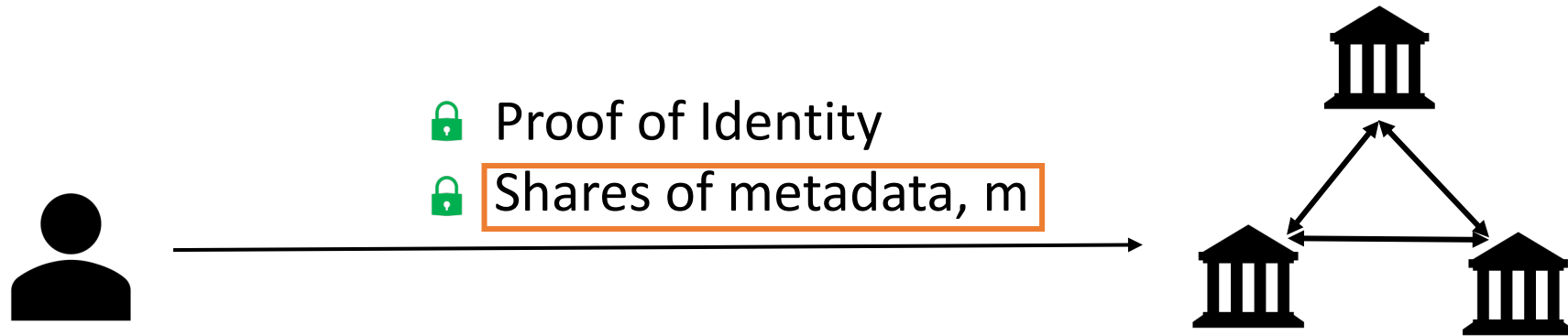
- A majority of escrows must cooperate to reveal m
- No minority of escrows have any information about m





At initialization, escrows secret share a random s that nobody knows

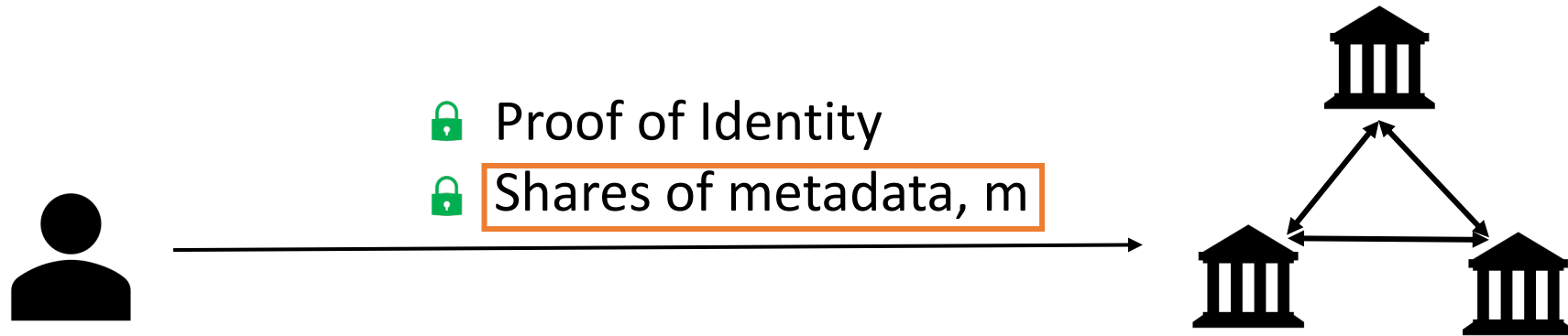
Distributed Allegation Escrow



At initialization, escrows secret share a random s that nobody knows

Distributed Allegation Escrow

Escrows compute $\text{PRF}_s(m)$



At initialization, escrows secret share a random s that nobody knows

Distributed Allegation Escrow

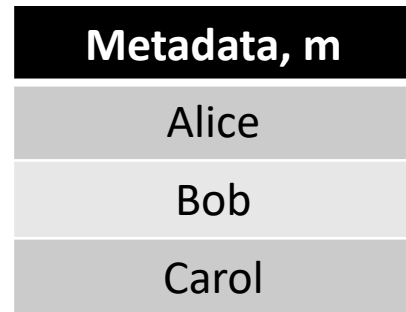
Escrows compute $\text{PRF}_s(m)$

Secure Multi-Party Computation (MPC)

Nobody learns m or s . Every escrow learns $\text{PRF}_s(m)$

If everybody had a threshold, $t = 2$


No escrows can see this
(ID of accused)



Metadata, m
Alice
Bob
Carol

If everybody had a threshold, $t = 2$


No escrows can see this
(ID of accused)



Metadata, m	Threshold
Alice	2
Bob	2
Carol	2

If everybody had a threshold, $t = 2$

No escrows can see this
(ID of accused)




Metadata, m	Threshold	$PRF_s(m)$
Alice	2	35318264c9a98faf
Bob	2	da6645f6e22bf5f7
Carol	2	6f90f1011151407

If everybody had a threshold, $t = 2$

No escrows can see this
(ID of accused)

All Escrows can see this



Metadata, m	Threshold	PRF _s (m)
Alice	2	35318264c9a98faf
Bob	2	da6645f6e22bf5f7
Carol	2	6f90f1011151407

If everybody had a threshold, $t = 2$

No escrows can see this
(ID of accused)

All Escrows can see this

Metadata, m	Threshold	$PRF_s(m)$
Alice	2	35318264c9a98faf
Bob	2	da6645f6e22bf5f7
Carol	2	6f90f1011151407

→ Looks random
Doesn't reveal information
Beyond equality/inequality

If everybody had a threshold, $t = 2$

No escrows can see this
(ID of accused)

All Escrows can see this

Metadata, m	Threshold	PRF _s (m)
Alice	2	35318264c9a98faf
Bob	2	da6645f6e22bf5f7
Carol	2	6f90f1011151407
Bob	2	da6645f6e22bf5f7



Match found!
Can be revealed

If everybody had a threshold, $t = 2$

No escrows can see this
(ID of accused)

All Escrows can see this

Metadata, m	Threshold	PRF _s (m)
Alice	2	35318264c9a98faf
Bob	2	da6645f6e22bf5f7
Carol	2	6f90f1011151407
Bob	2	da6645f6e22bf5f7

Match found!
Can be revealed

~~$O(N)$ = Not Scalable~~

$O(1)$ = Scalable!

If everybody had a threshold, $t = 2$

No escrows can see this
(ID of accused)

All Escrows can see this

Metadata, m	Threshold	PRF _s (m)
Alice	2	35318264c9a98faf
Bob	2	da6645f6e22bf5f7
Carol	2	6f90f1011151407
Bob	2	da6645f6e22bf5f7

Match found!
Can be revealed

Adversary cannot compare allegations on its own

At least one honest escrow must cooperate to compute PRF_s(m)

If everybody had a threshold, $t = 2$

No escrows can see this
(ID of accused)

All Escrows can see this

Metadata, m	Threshold	PRF _s (m)
Alice	2	35318264c9a98faf
Bob	2	da6645f6e22bf5f7
Carol	2	6f90f1011151407
Bob	2	da6645f6e22bf5f7

Match found!
Can be revealed

Adversary cannot compare allegations on its own

At least one honest escrow must cooperate to compute PRF_s(m)

Hence, allegor must submit a proof of identity to that honest escrow.

Forces adversary to leave a paper trail

Thresholds $t \geq 2$

No escrows can see this
(ID of accused)

All Escrows can see this

Metadata, m	Threshold	$\text{PRF}_s(m)$
Alice	2	35318264c9a98faf
Bob	2	da6645f6e22bf5f7
Carol	2	6f90f1011151407



Alice

Is there an allegation
against me?

Thresholds ≥ 2

No escrows can see this
(ID of accused)

All Escrows can see this

Metadata, m	Threshold	PRF _s (m)
Alice	2	35318264c9a98faf
Bob	2	da6645f6e22bf5f7
Carol	2	6f90f1011151407
Alice	100	35318264c9a98faf

Probe allegation



Alice

Is there an allegation
against me?

Won't be revealed
Not bad for Alice

Thresholds ≥ 2

No escrows can see this
(ID of accused)

All Escrows can see this

Metadata, m	Threshold	PRF _s (m)
Alice	2	35318264c9a98faf
Bob	2	da6645f6e22bf5f7
Carol	2	6f90f1011151407
Alice	100	35318264c9a98faf

All escrows know
these are equal

Probe allegation



Alice

Is there an allegation
against me?

Won't be revealed
Not bad for Alice

Thresholds ≥ 2

No escrows can see this
(ID of accused)

All Escrows can see this

Metadata, m	Threshold	PRF _s (m)
Alice	2	35318264c9a98faf
Bob	2	da6645f6e22bf5f7
Carol	2	6f90f1011151407
Alice	100	35318264c9a98faf

All escrows know
these are equal

Alice has corrupted one escrow.
Hence she knows there is one
allegation against her

Probe allegation

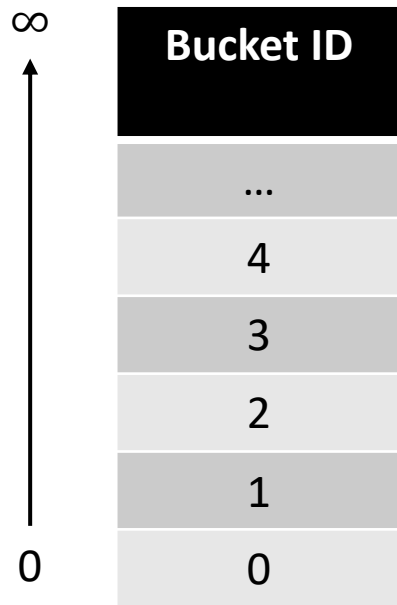
Is there an allegation
against me?

Won't be revealed
Not bad for Alice

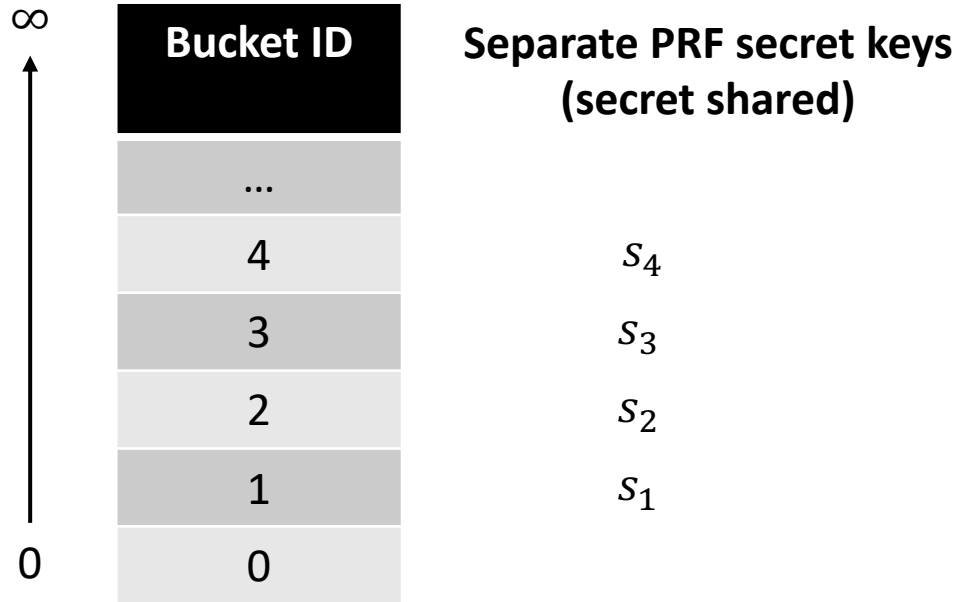


Alice

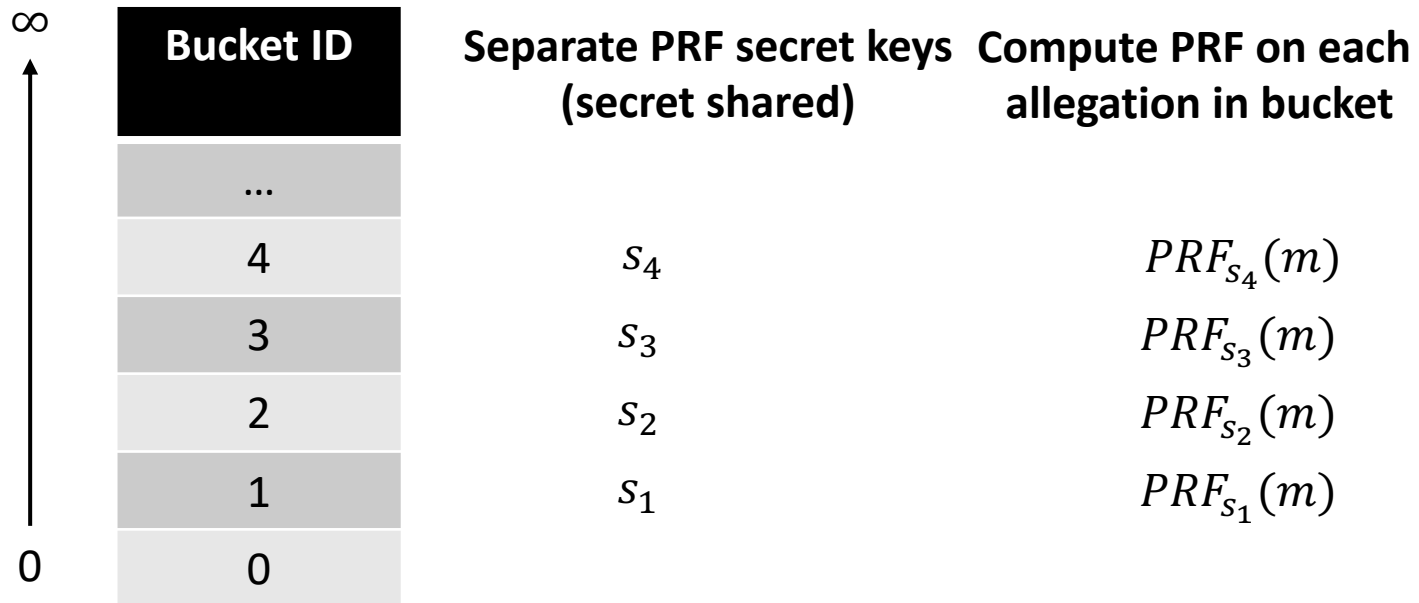
Bucketing Protocol



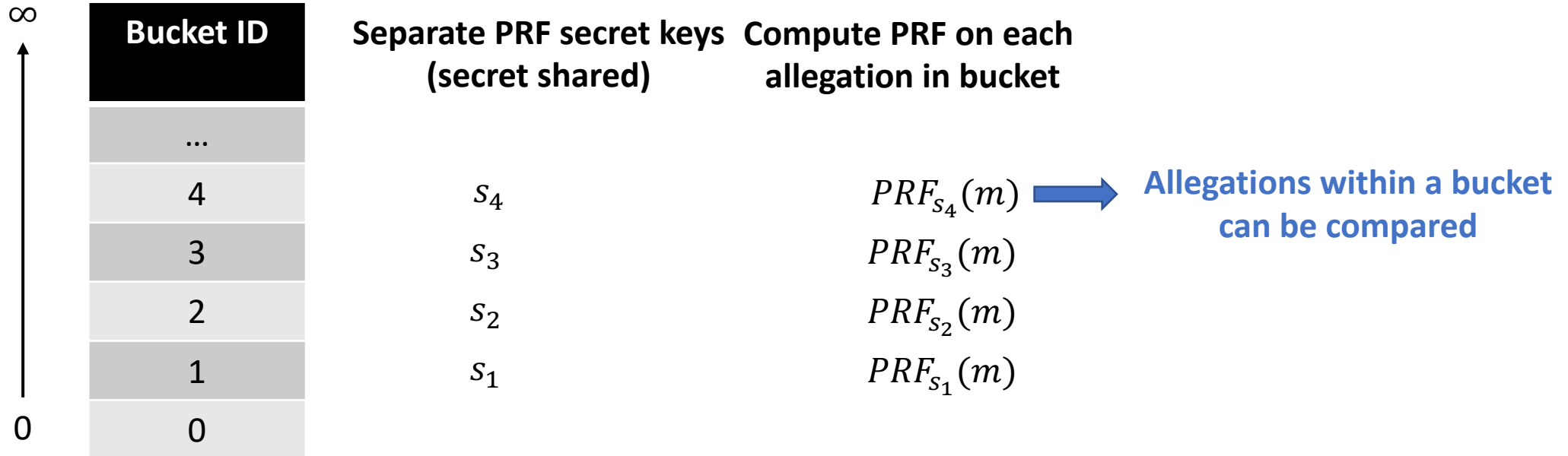
Bucketing Protocol



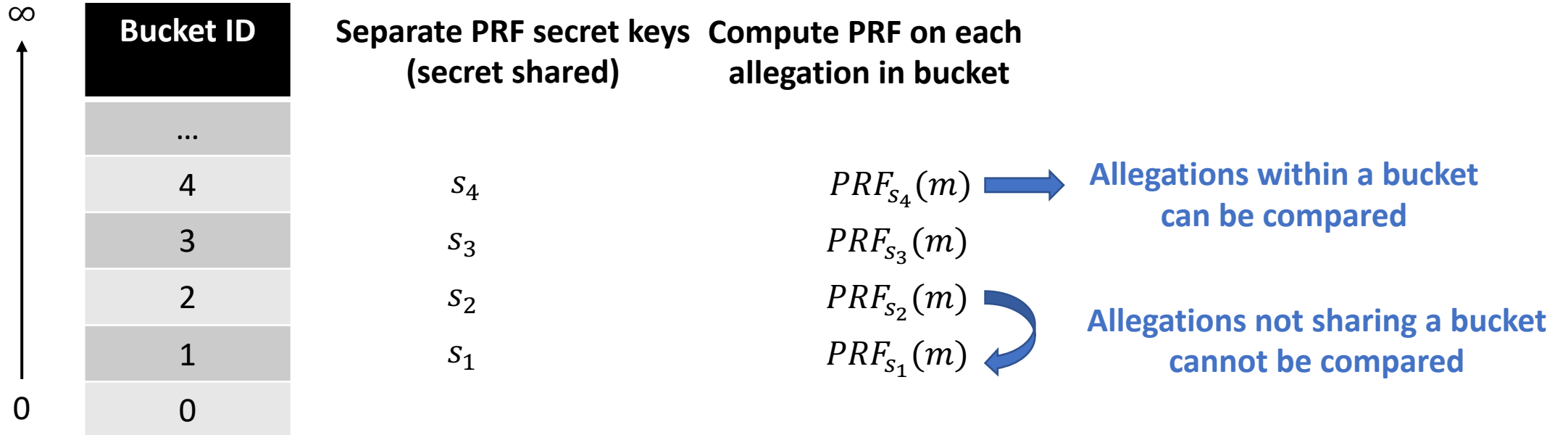
Bucketing Protocol



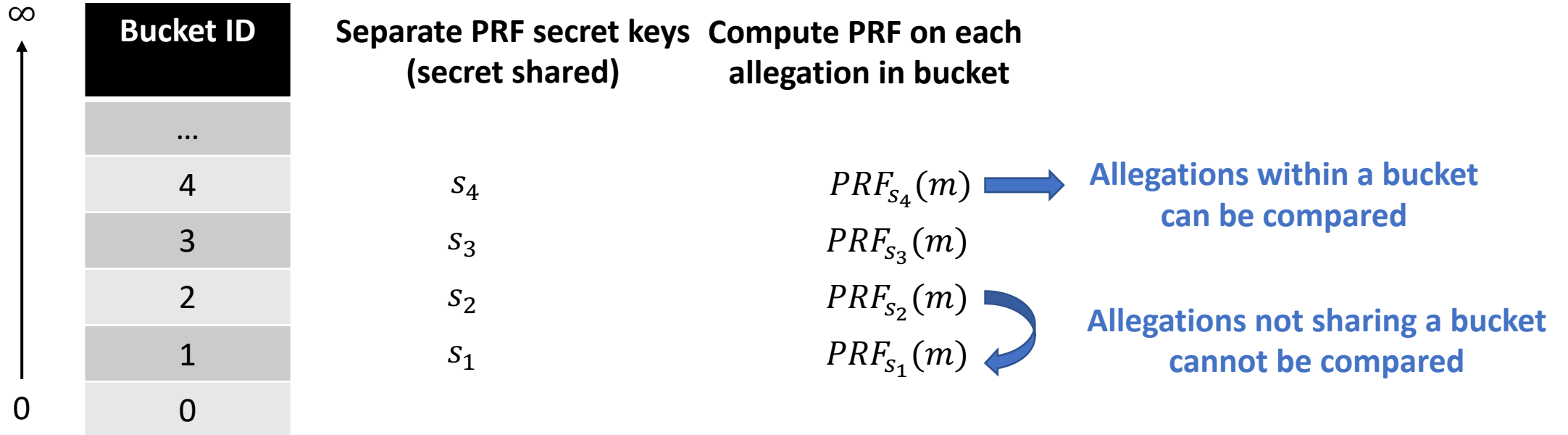
Bucketing Protocol



Bucketing Protocol

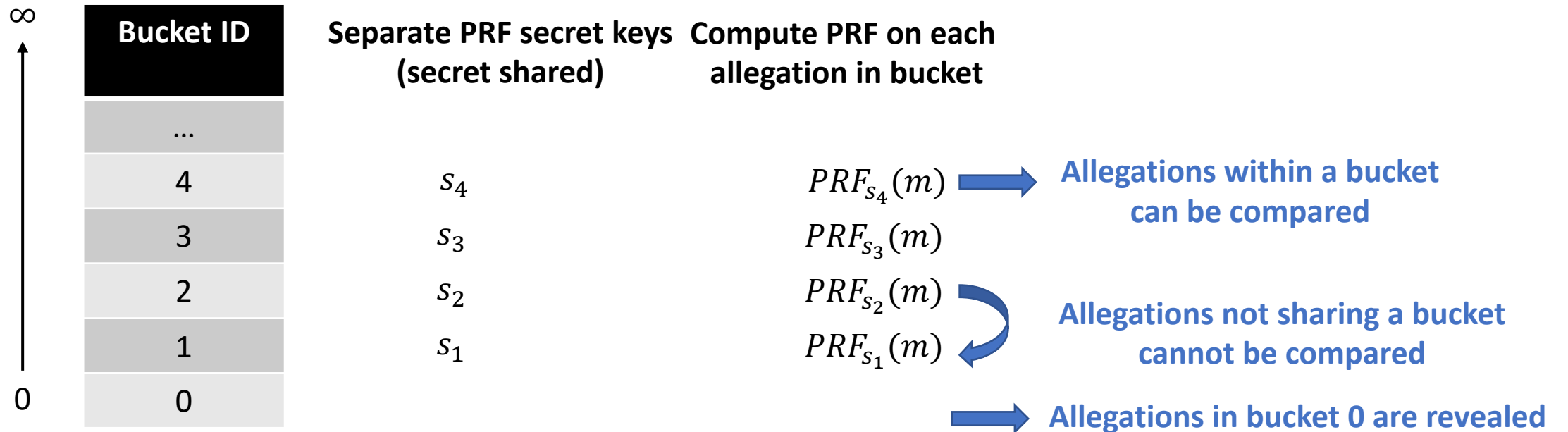


Bucketing Protocol



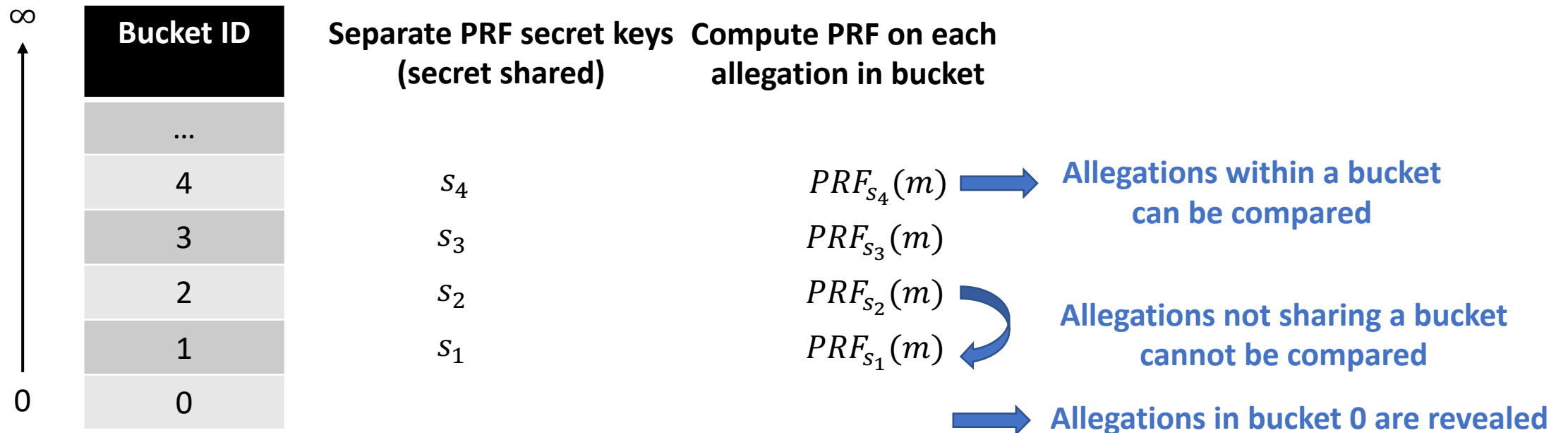
Invariant
An allegation is in bucket i if i more allegations will cause it to be revealed

Bucketing Protocol



Invariant
An allegation is in bucket i if i more allegations will cause it to be revealed

Bucketing Protocol

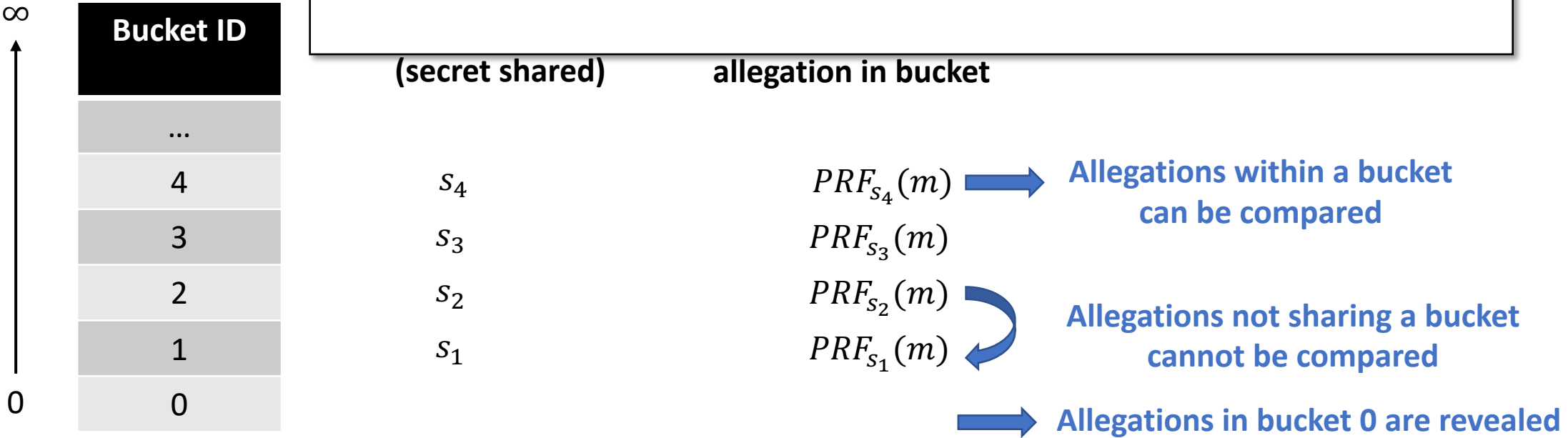


Invariant
 An allegation is in bucket i if i more allegations will cause it to be revealed

Key Property
 Allegations that have been compared, will be revealed together if at all

Bucketing Protocol

If probe allegation matches an honest allegation:



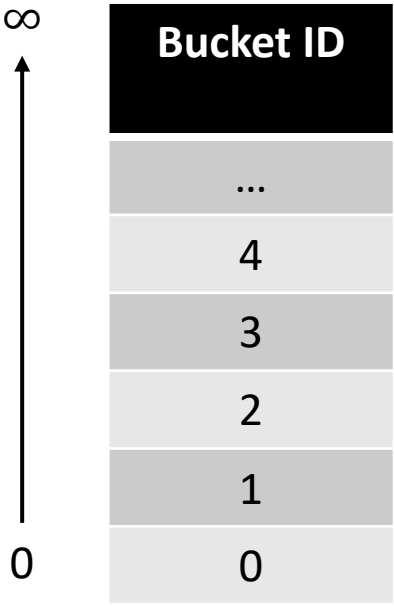
Invariant
An allegation is in bucket i if i more allegations will cause it to be revealed

Key Property
Allegations that have been compared, will be revealed together if at all

Bucketing Protocol

If probe allegation matches an honest allegation:

- Probe allegation is just as likely to be revealed as the honest one



(secret shared) allegation in bucket

s_4
 s_3
 s_2
 s_1

$PRF_{s_4}(m)$
 $PRF_{s_3}(m)$
 $PRF_{s_2}(m)$
 $PRF_{s_1}(m)$

Allegations within a bucket can be compared

Allegations not sharing a bucket cannot be compared

Allegations in bucket 0 are revealed

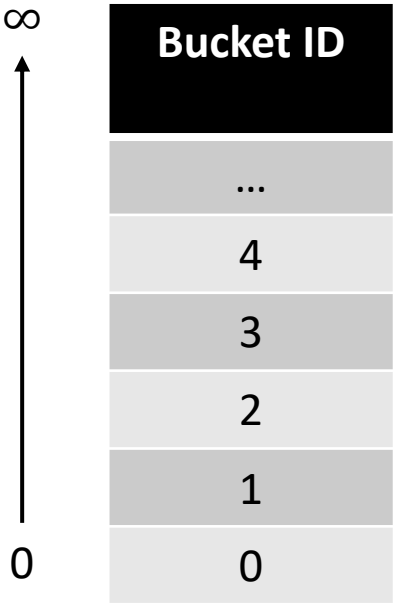
Invariant
An allegation is in bucket i if i more allegations will cause it to be revealed

Key Property
Allegations that have been compared, will be revealed together if at all

Bucketing Protocol

If probe allegation matches an honest allegation:

- Probe allegation is just as likely to be revealed as the honest one
- Honest allegation is now waiting for one less allegation



(secret shared) allegation in bucket

s_4
 s_3
 s_2
 s_1

$PRF_{s_4}(m)$
 $PRF_{s_3}(m)$
 $PRF_{s_2}(m)$
 $PRF_{s_1}(m)$

Allegations within a bucket can be compared


Allegations not sharing a bucket cannot be compared

Allegations in bucket 0 are revealed

Invariant
An allegation is in bucket i if i more allegations will cause it to be revealed

Key Property
Allegations that have been compared, will be revealed together if at all



Bucketing Protocol

Bucket ID	Allegation 1 $t = 6$
5	
4	
3	
2	
1	
0	

Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed

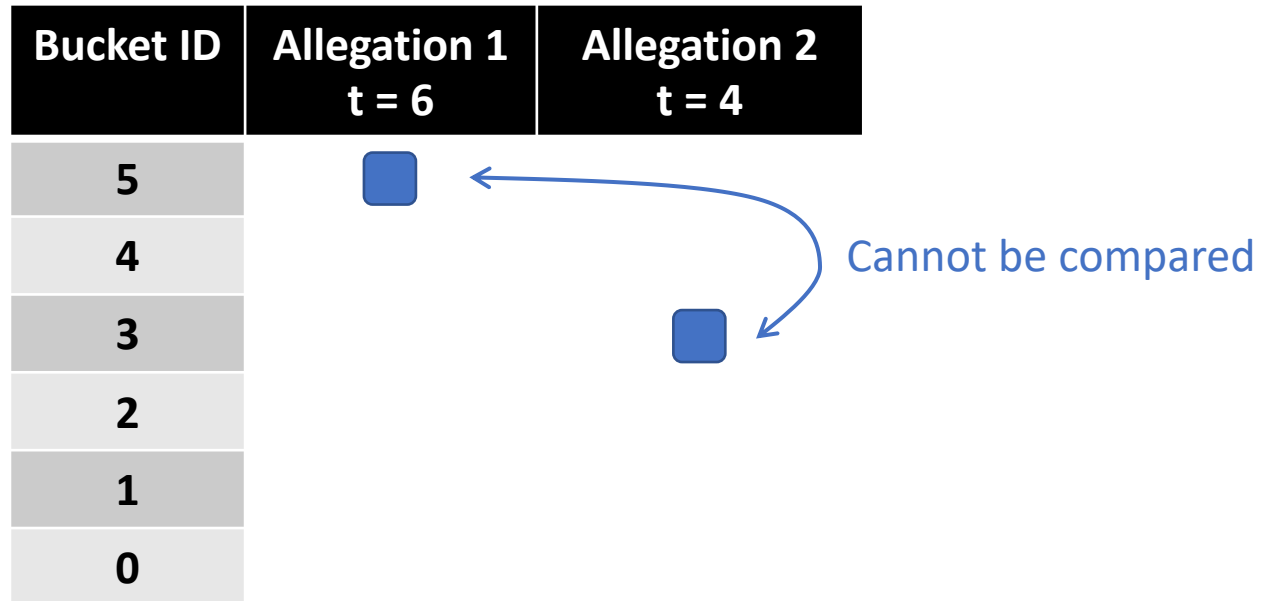
Bucketing Protocol

Bucket ID	Allegation 1 $t = 6$	Allegation 2 $t = 4$
5		
4		
3		
2		
1		
0		

Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed




Bucketing Protocol



Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed




Bucketing Protocol

Bucket ID	Allegation 1 $t = 6$	Allegation 2 $t = 4$	Allegation 3 $t = 4$
5			
4			
3			
2			
1			
0			

Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed

Bucketing Protocol



Bucket ID	Allegation 1 $t = 6$	Allegation 2 $t = 4$	Allegation 3 $t = 4$
5			
4			
3			
2			
1			
0			

Can be compared

Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed



Bucketing Protocol

Bucket ID	Allegation 1 $t = 6$	Allegation 2 $t = 4$	Allegation 3 $t = 4$
5			
4			
3			
2			
1			
0			

Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed

Bucketing Protocol

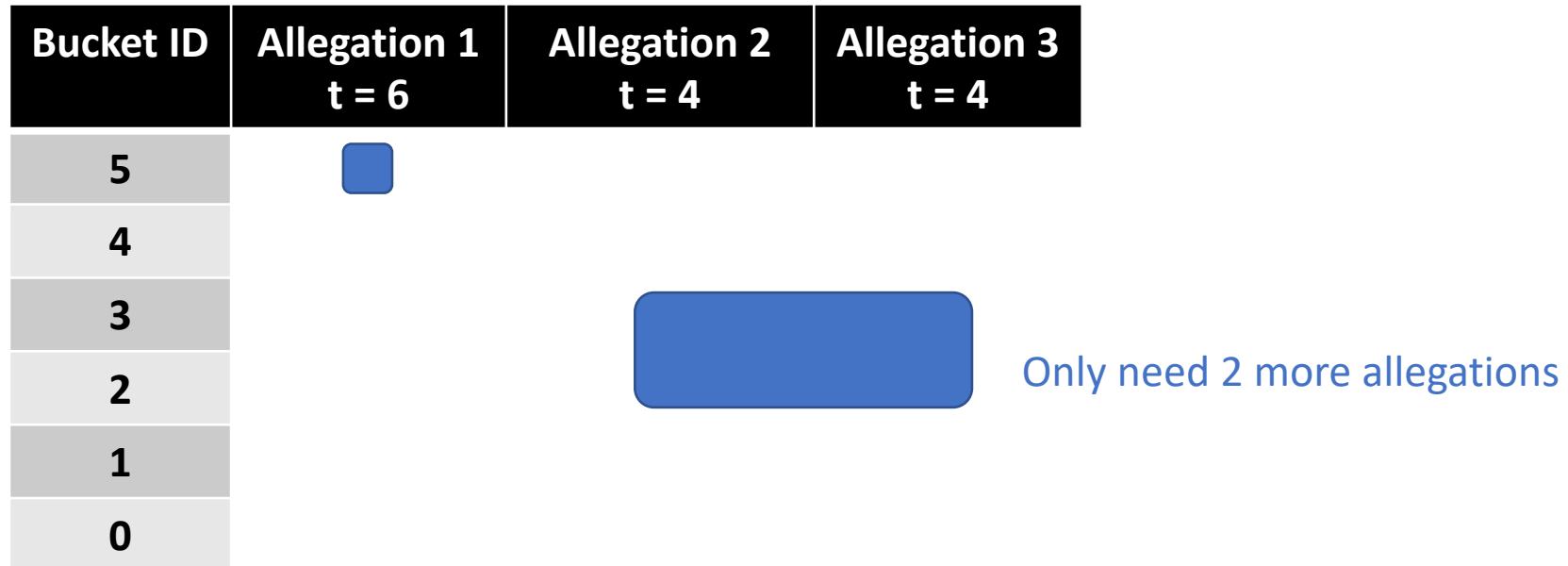
Bucket ID	Allegation 1 $t = 6$	Allegation 2 $t = 4$	Allegation 3 $t = 4$
5			
4			
3			
2			
1			
0			

Collection of 2 allegations
waiting for the same number
of matching allegations

Invariant

An allegation is in bucket i if i more
allegations will cause it to be revealed

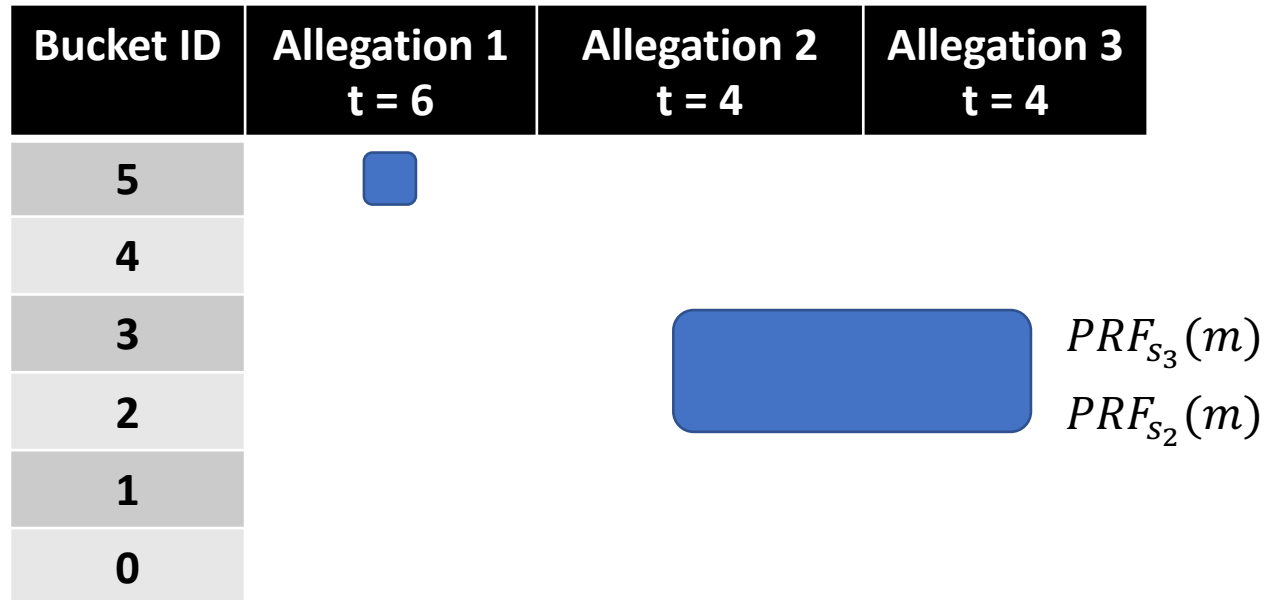
Bucketing Protocol



Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed




Bucketing Protocol



Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed

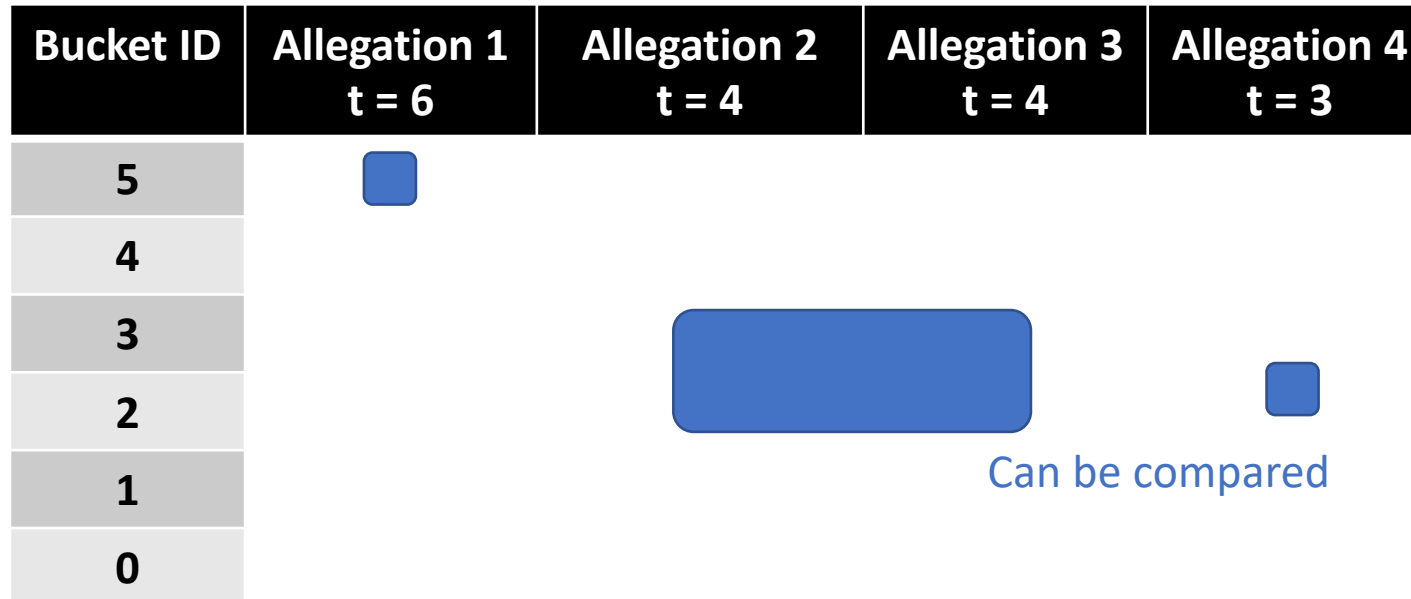
Bucketing Protocol

Bucket ID	Allegation 1 $t = 6$	Allegation 2 $t = 4$	Allegation 3 $t = 4$	Allegation 4 $t = 3$
5				
4				
3				
2				
1				
0				

Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed



Bucketing Protocol



Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed



Bucketing Protocol

Bucket ID	Allegation 1 $t = 6$	Allegation 2 $t = 4$	Allegation 3 $t = 4$	Allegation 4 $t = 3$
5				
4				
3				
2				
1				
0				

Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed




Bucketing Protocol

Bucket ID	Allegation 1 $t = 6$	Allegation 2 $t = 4$	Allegation 3 $t = 4$	Allegation 4 $t = 3$
5				
4				
3				
2				
1				
0				

Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed

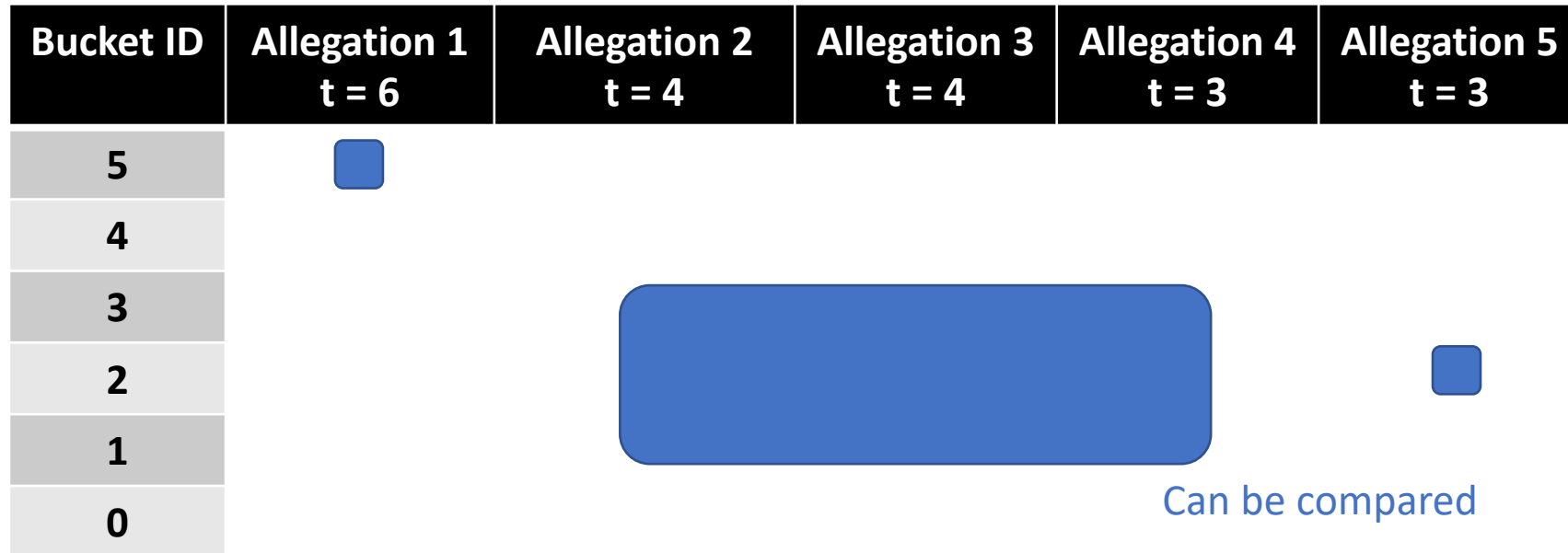
Bucketing Protocol

Bucket ID	Allegation 1 $t = 6$	Allegation 2 $t = 4$	Allegation 3 $t = 4$	Allegation 4 $t = 3$	Allegation 5 $t = 3$
5					
4					
3					
2					
1					
0					

Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed


Bucketing Protocol




Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed

Bucketing Protocol


Bucket ID	Allegation 1 $t = 6$	Allegation 2 $t = 4$	Allegation 3 $t = 4$	Allegation 4 $t = 3$	Allegation 5 $t = 3$
5					
4					
3					
2					
1					
0					




Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed

Bucketing Protocol



Bucket ID	Allegation 1 $t = 6$	Allegation 2 $t = 4$	Allegation 3 $t = 4$	Allegation 4 $t = 3$	Allegation 5 $t = 3$
5					
4					
3					
2					
1					
0					



Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed

Bucketing Protocol



Bucket ID	Allegation 1 $t = 6$	Allegation 2 $t = 4$	Allegation 3 $t = 4$	Allegation 4 $t = 3$	Allegation 5 $t = 3$
5					
4					
3					
2					
1					
0					

 Revealed

Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed

Bucketing Protocol

Bucket ID	Allegation 1 t = 6	Allegation 2 t = 4	Allegation 3 t = 4	Allegation 4 t = 3	Allegation 5 t = 3
5					
4					
3					
2					
1					
0					


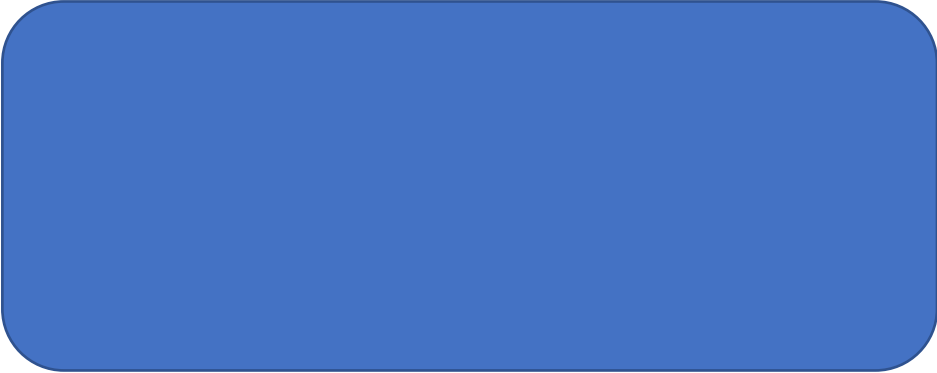
→ Not Revealed

→ Revealed

Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed

Bucketing Protocol

Bucket ID	Allegation 1 t = 6	Allegation 2 t = 4	Allegation 3 t = 4	Allegation 4 t = 3	Allegation 5 t = 3
5					
4					
3					
2					
1					
0					


→ Not Revealed

→ Revealed

Invariant

An allegation is in bucket i if i more allegations will cause it to be revealed

Bucketing Protocol

Bucket ID	Allegation 1 $t = 6$	Allegation 2 $t = 4$	Allegation 3 $t = 4$	Allegation 4 $t = 3$	Allegation 5 $t = 3$
5					
4					
3					
2					
1					
0					

→ Not Revealed

Efficiency
In an amortized sense, each allegation requires 2 PRF computations

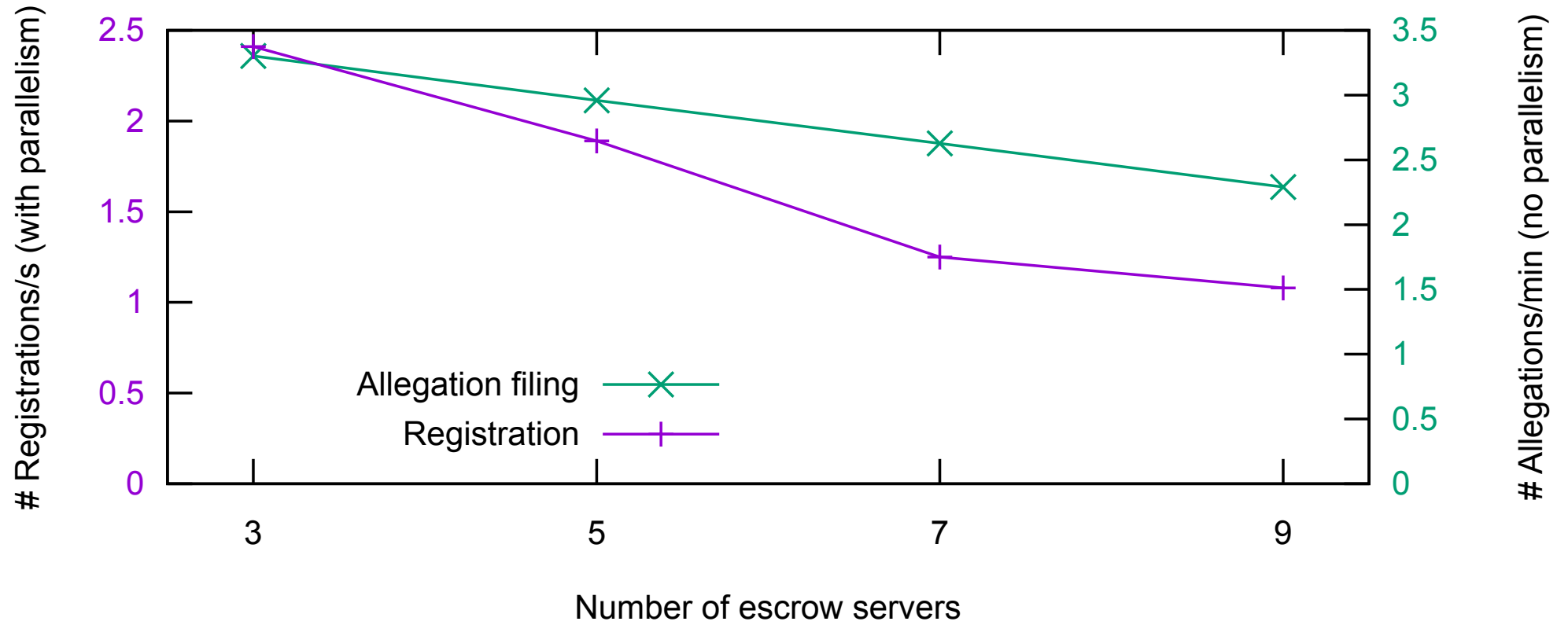
→ Revealed

Invariant
An allegation is in bucket i if i more allegations will cause it to be revealed

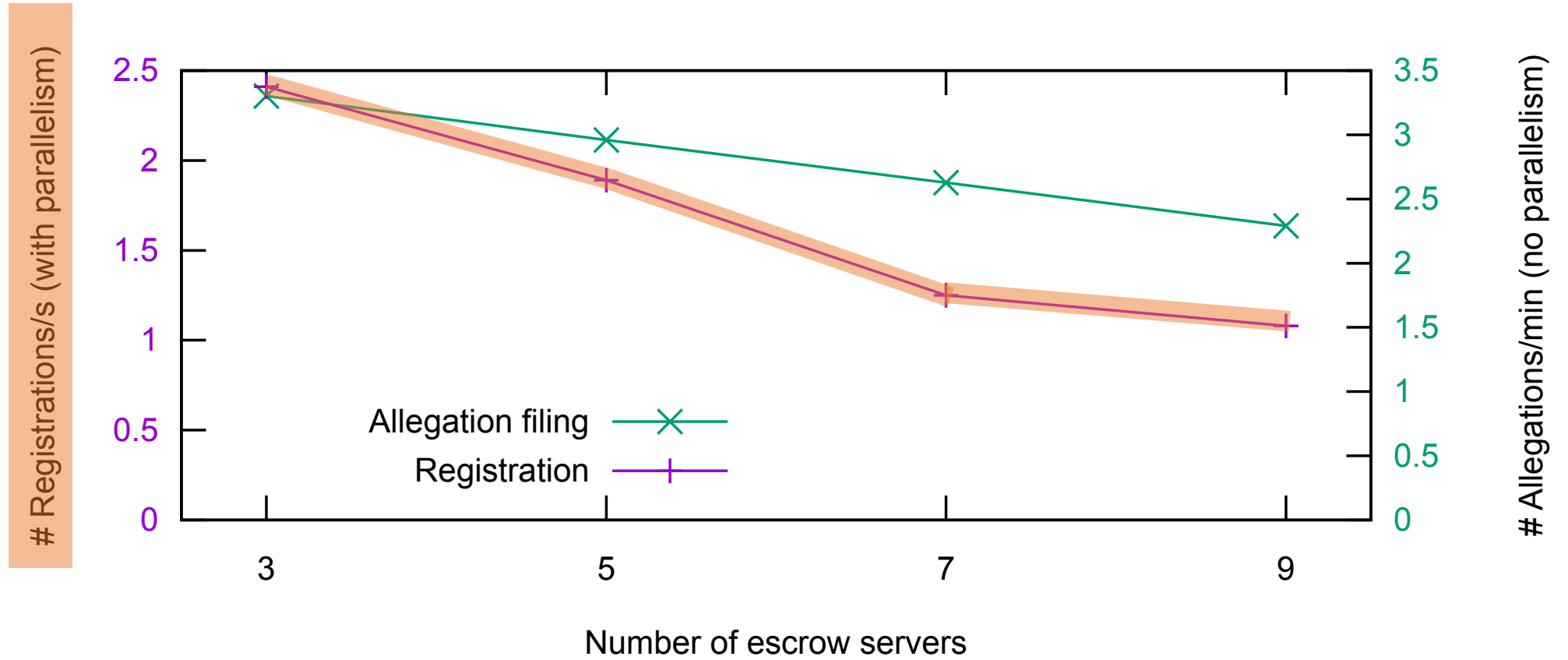
Security in the UC model

See paper for details

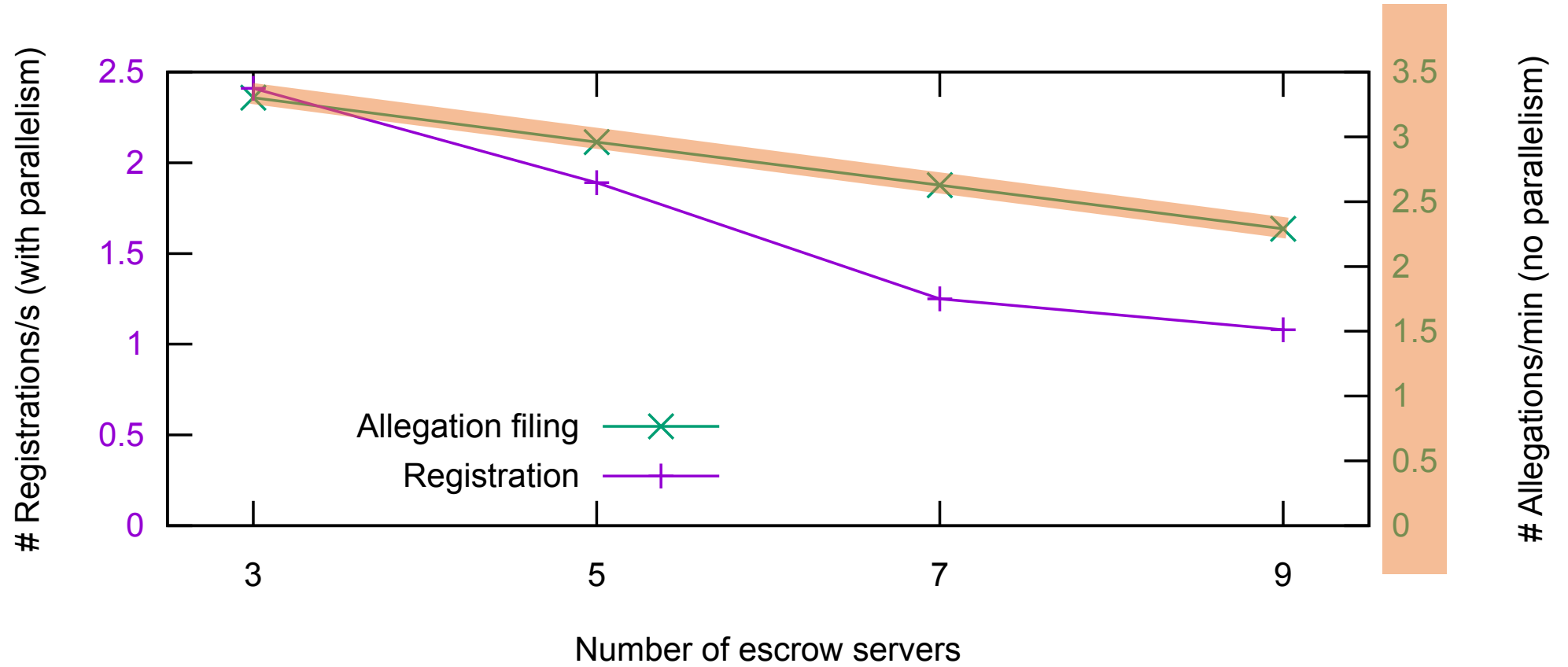
Evaluation



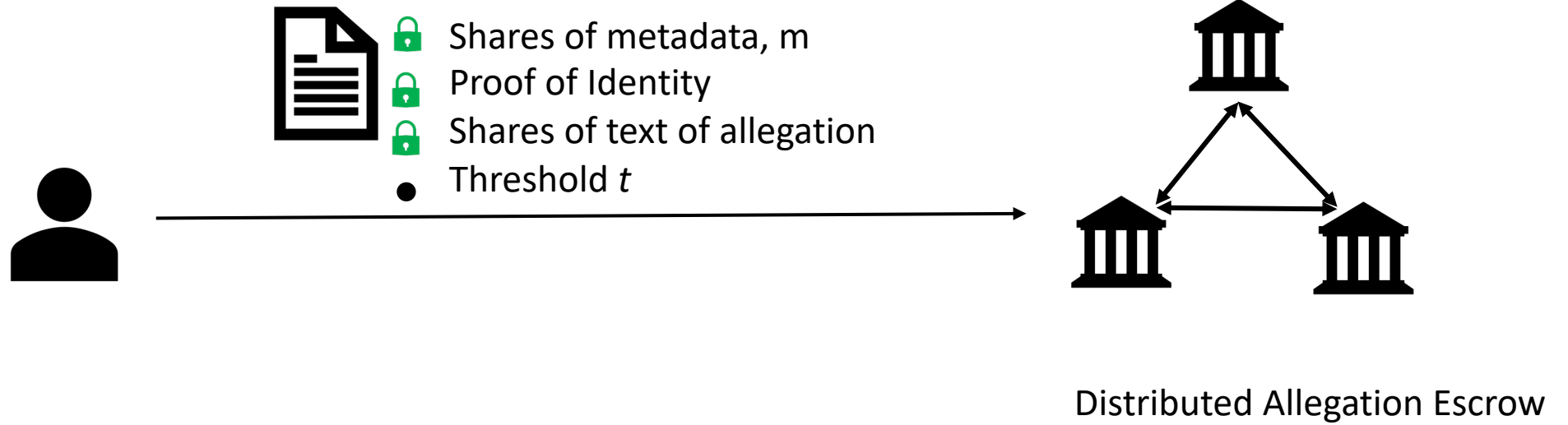
Evaluation



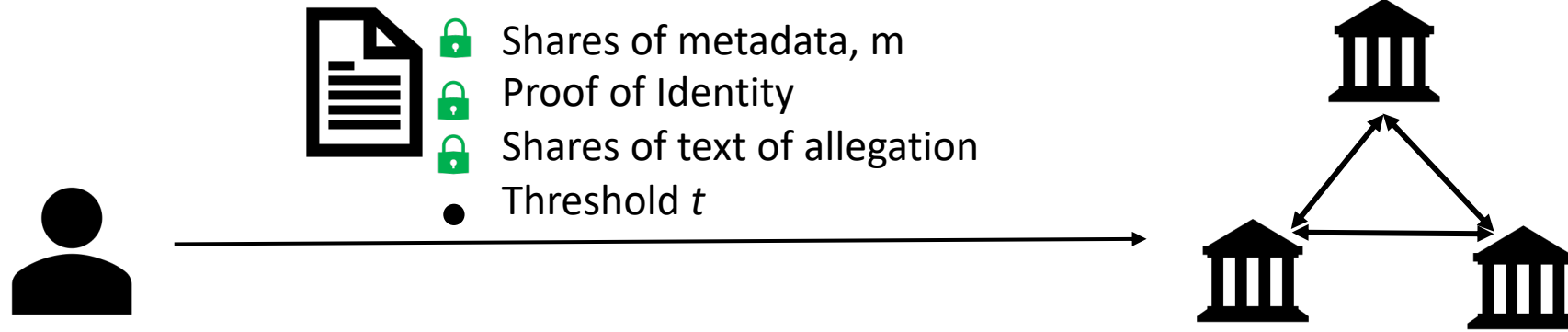
Evaluation



Summary



Summary



Distributed Allegation Escrow

Reveal **identity** and **text**
only as part of a group of size at-least **t**