Perfect (Parallel) Broadcast in Constant Expected Time via Statistical VSS

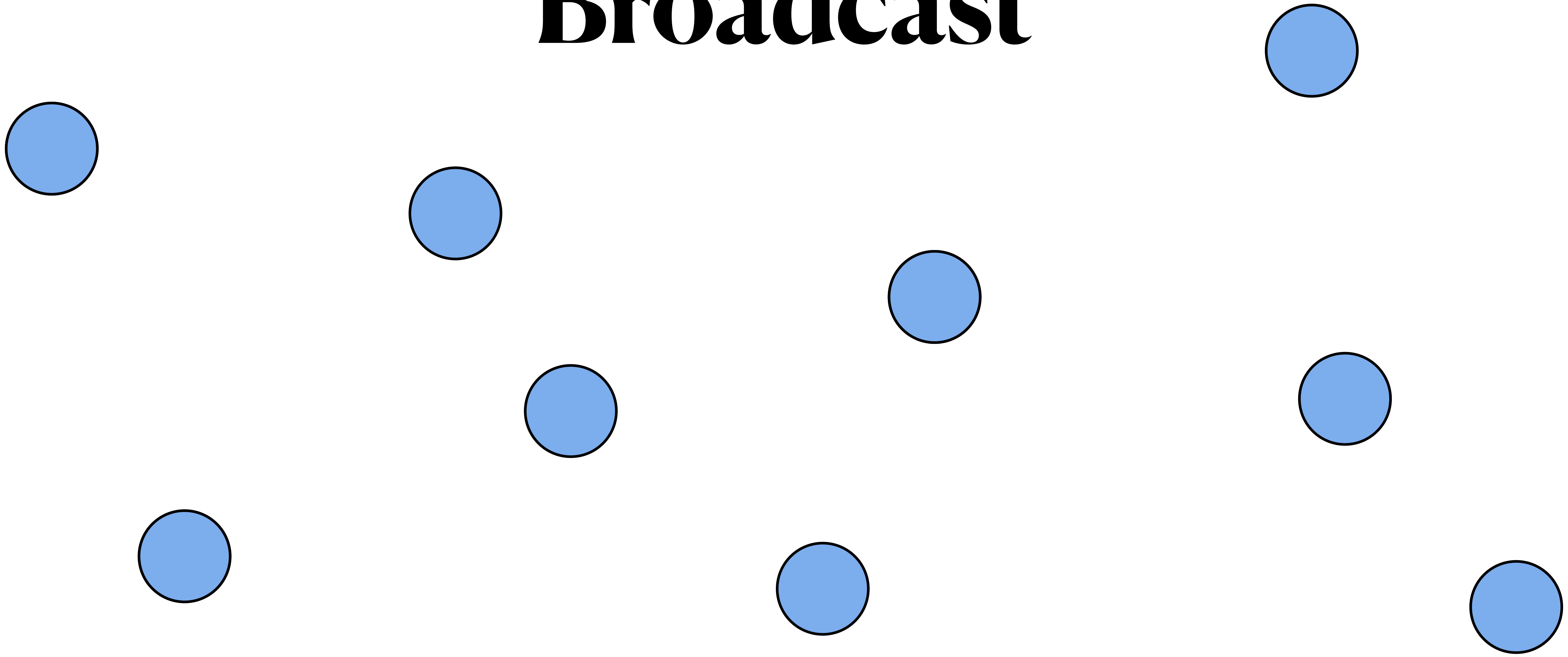
Gilad Asharov

Anirudh Chandramouli

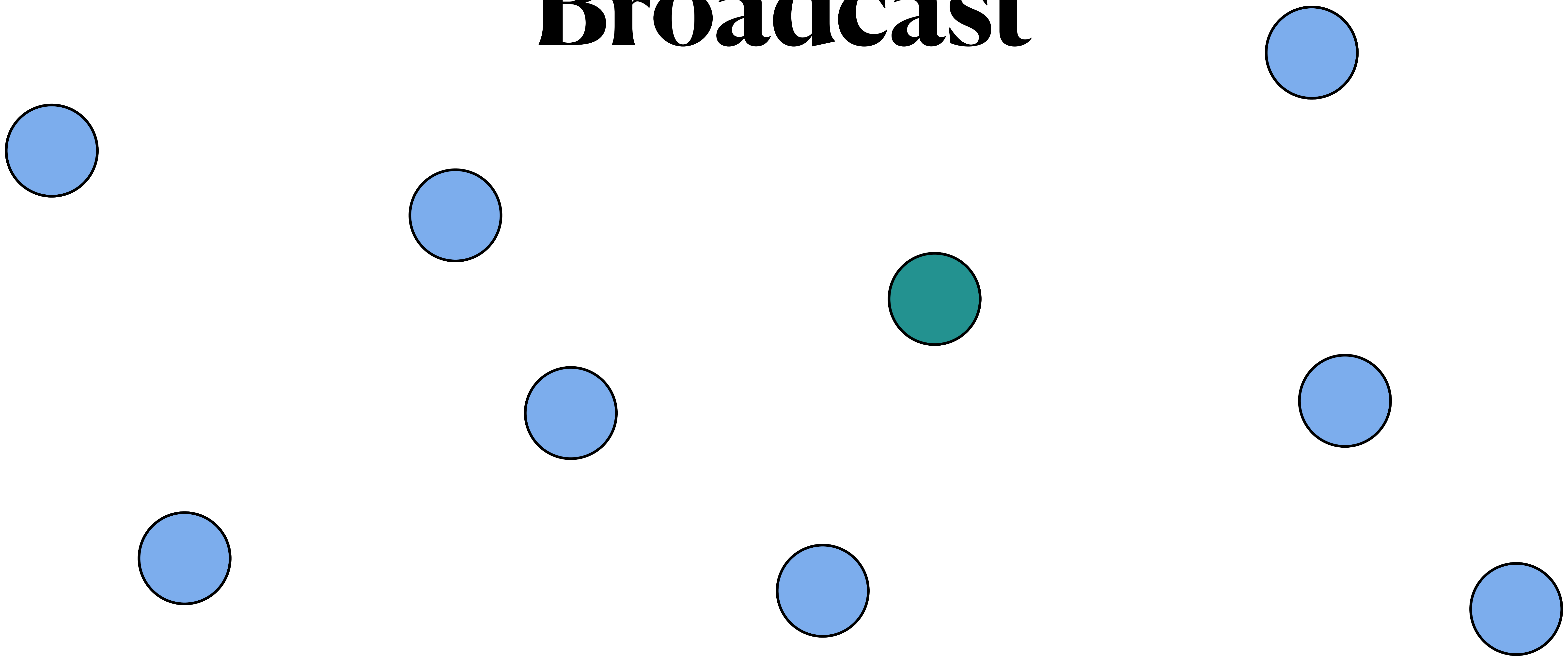
Bar-Ilan University

Center for Research in Applied Cryptography and Cyber Security

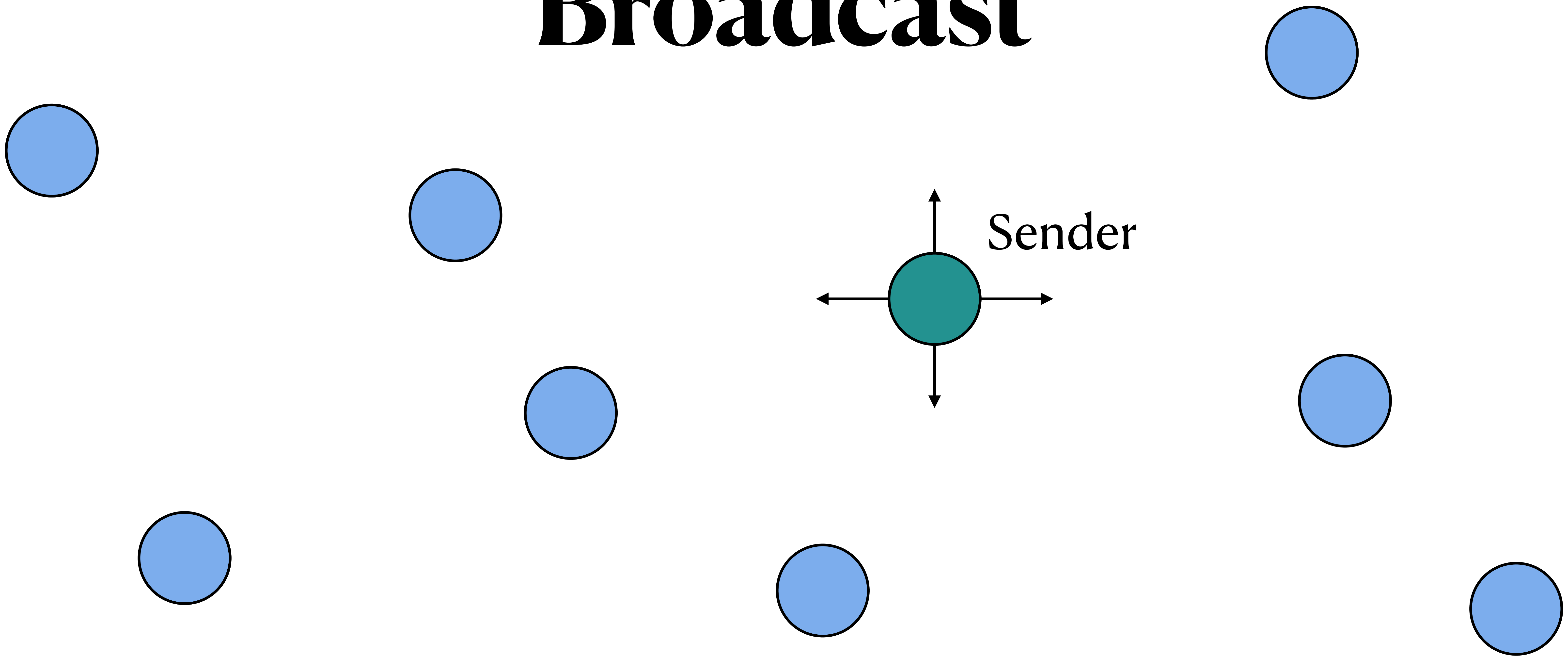
Broadcast



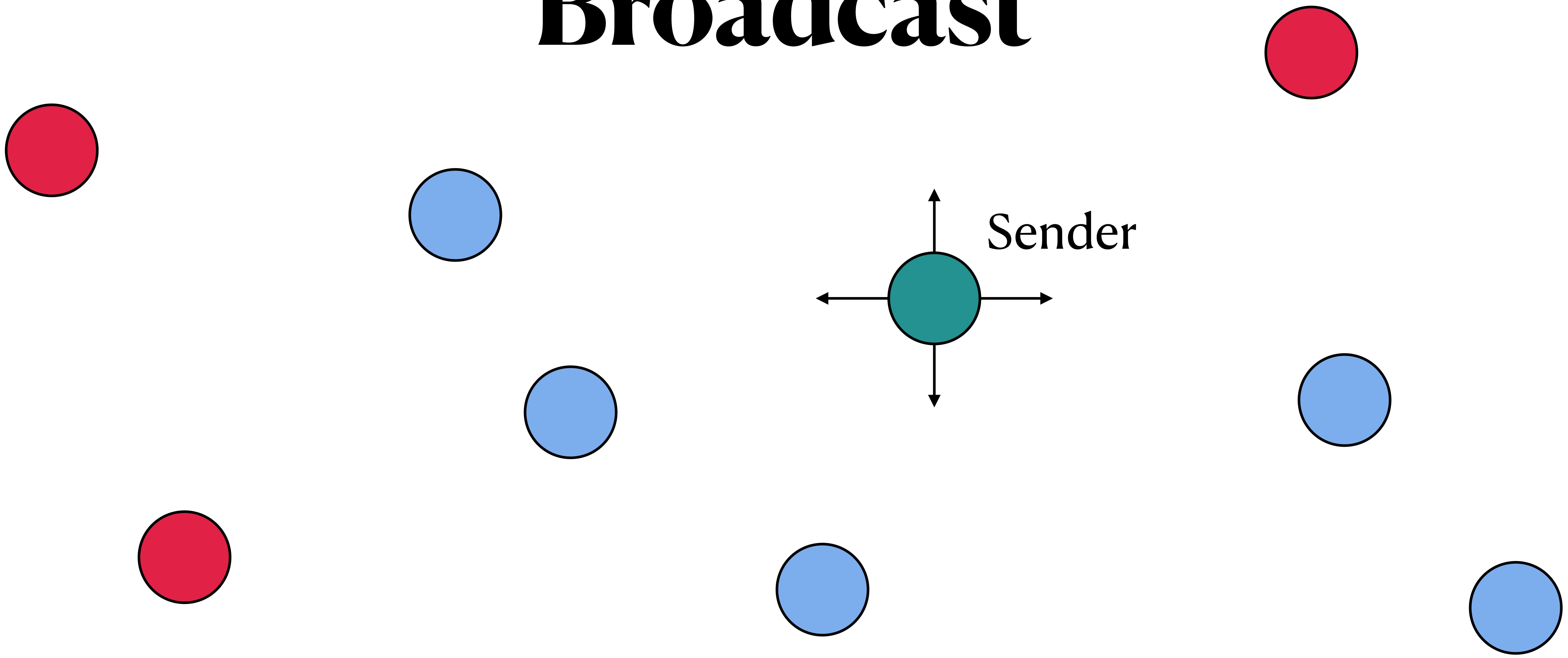
Broadcast



Broadcast

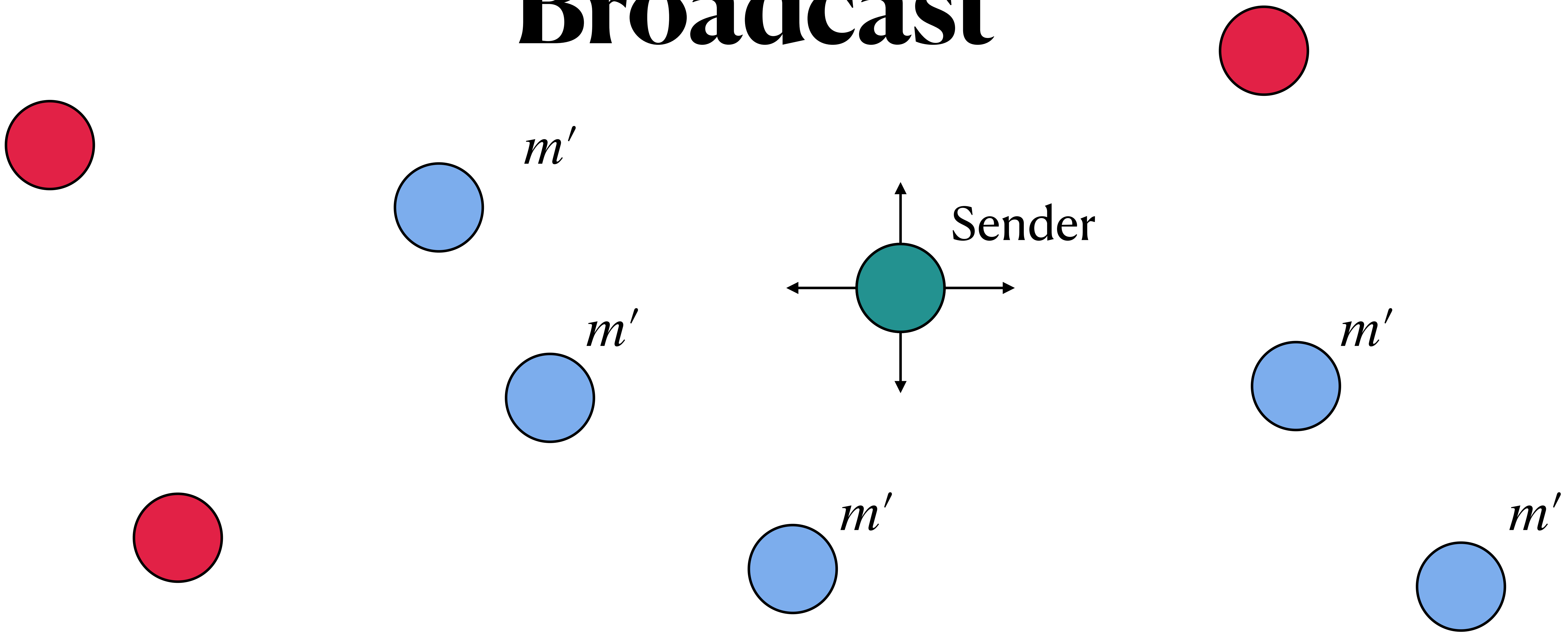


Broadcast



t corrupted parties/sender may deceive the honest parties

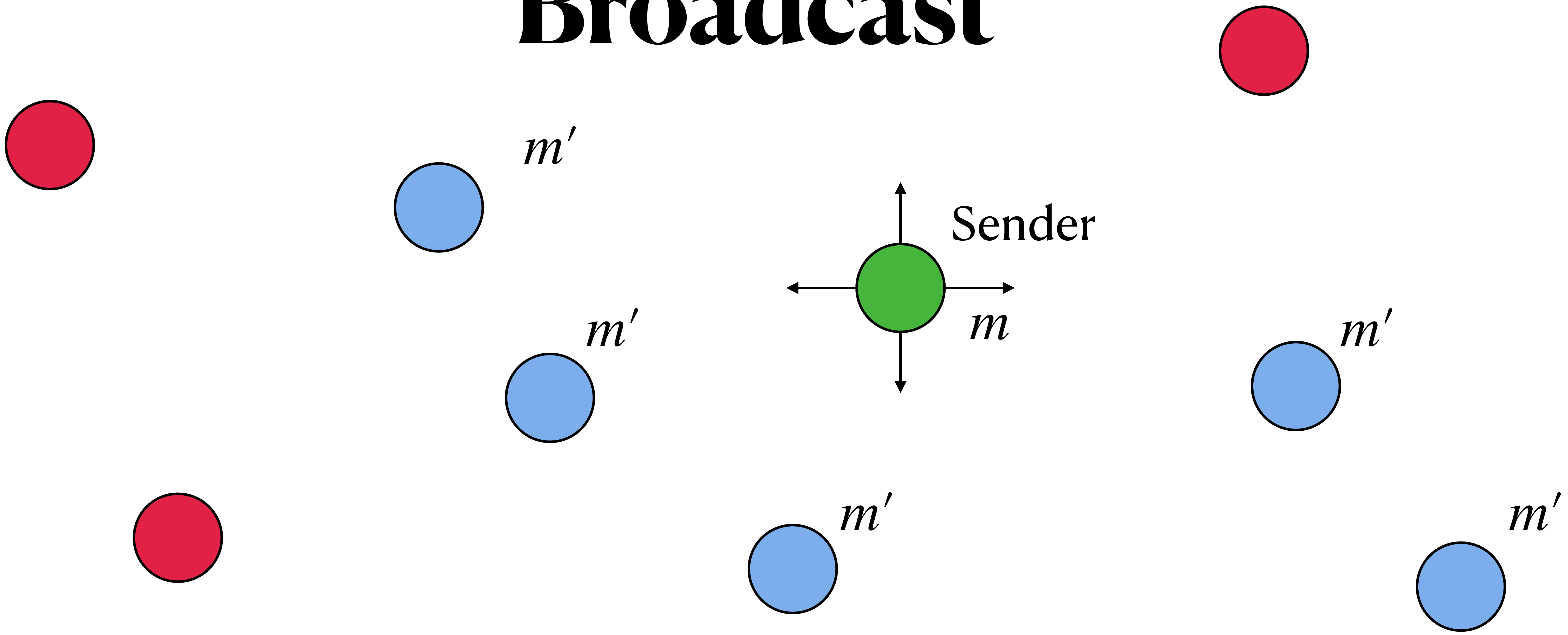
Broadcast



t corrupted parties/sender may deceive the honest parties

- **Agreement:** Everyone outputs the same message *m’*

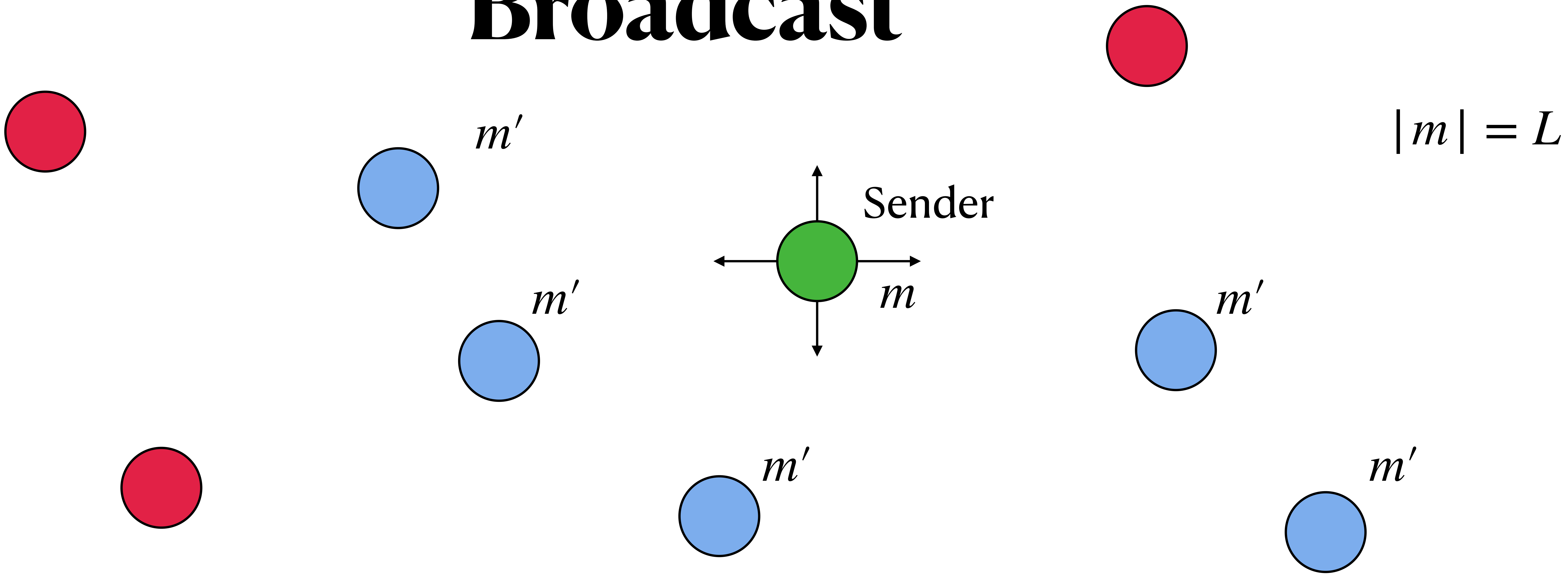
Broadcast



t corrupted parties/sender may deceive the honest parties

- **Agreement:** Everyone outputs the same message *m'*
- **Validity:** For honest sender *m'=m*

Broadcast



t corrupted parties/sender may deceive the honest parties

- **Agreement:** Everyone outputs the same message *m'*
- **Validity:** For honest sender *m'*=*m*

Setting

Setting

- Realize broadcast on ideal pair-wise private and authenticated channels
- No computational hardness assumptions
- Zero probability of error

Setting

- Realize broadcast on ideal pair-wise private and authenticated channels
- No computational hardness assumptions
- Zero probability of error

Lower Bounds

Setting

- Realize broadcast on ideal pair-wise private and authenticated channels
- No computational hardness assumptions
- Zero probability of error

Lower Bounds

- **Resilience:** $t < n/3$ is necessary [PSL80,LSP82]
- **Rounds:** Deterministic $\Omega(n)$ [FL82]
- **Communication:** $\Omega(n^2)$ messages [DR82] (also [ACD+23])

Setting

- Realize broadcast on ideal pair-wise private and authenticated channels
- No computational hardness assumptions
- Zero probability of error

Lower Bounds

$n \geq 3t + 1$

- **Resilience:** $t < n/3$ is necessary [PSL80,LSP82]
- **Rounds:** Deterministic $\Omega(n)$ [FL82]
- **Communication:** $\Omega(n^2)$ messages [DR82] (also [ACD+23])

Setting

- Realize broadcast on ideal pair-wise private and authenticated channels
- No computational hardness assumptions
- Zero probability of error

Lower Bounds

- **Resilience:** $t < n/3$ is necessary [PSL80,LSP82]
- **Rounds:** Deterministic $\Omega(n)$ [FL82]
- **Communication:** $\Omega(n^2)$ messages [DR82] (also [ACD+23])

$n \geq 3t + 1$

$\mathsf{E}(O(1))$

Setting

- Realize broadcast on ideal pair-wise private and authenticated channels
- No computational hardness assumptions
- Zero probability of error

Lower Bounds

- **Resilience:** $t < n/3$ is necessary [PSL80,LSP82]
- **Rounds:** Deterministic $\Omega(n)$ [FL82]
- **Communication:** $\Omega(n^2)$ messages [DR82] (also [ACD+23])

$n \geq 3t + 1$

$\mathsf{E}(O(1))$

$O(nL + n^2)$

State of the Art: Broadcast

State of the Art: Broadcast

Succinct with High Latency

State of the Art: Broadcast

Succinct with High Latency

More Comm. but with expected Low Latency

State of the Art: Broadcast

Succinct with High Latency

More Comm. but with expected Low Latency

Communication

Rounds

State of the Art: Broadcast

Succinct with High Latency

More Comm. but with expected Low Latency

Communication

$O(nL + n^2 \log n)$

Rounds

$\Omega(n)$

State of the Art: Broadcast

Succinct with High Latency

More Comm. but with expected Low Latency

Communication

[CW89], [BGP92] + [Che21]

$O(nL + n^2 \log n)$

Rounds

$\Omega(n)$

State of the Art: Broadcast

	Succinct with High Latency	More Comm. but with expected Low Latency
	[CW89], [BGP92] + [Che21]	[FM88]
Communication	$O(nL + n^2 \log n)$	$O(n^2L) + \mathrm{E}(\mathrm{poly}(n))$
Rounds	$\Omega(n)$	$\mathrm{E}(O(1))$

State of the Art: Broadcast

	Succinct with High Latency	More Comm. but with expected Low Latency	
Communication			
		$O(n^2 L) + \mathsf{E}(\text{poly}(n))$	[FM88]
[CW89], [BGP92] + [Che21]	$O(nL + n^2 \log n)$	$O(n^2 L) + \mathsf{E}(O(n^6 \log n))$	[KK06]
Rounds			
	$\Omega(n)$	$\mathsf{E}(O(1))$	

State of the Art: Broadcast

	Succinct with High Latency	More Comm. but with expected Low Latency	
Communication			
[CW89], [BGP92] + [Che21]	$O(nL + n^2 \log n)$	$O(n^2L) + \mathsf{E}(\text{poly}(n))$	[FM88]
		$O(n^2L) + \mathsf{E}(O(n^6 \log n))$	[KK06]
		$O(nL) + \mathsf{E}(O(n^4 \log n))$	[AAPP22]
Rounds			
	$\Omega(n)$	$\mathsf{E}(O(1))$	

State of the Art: Broadcast

	Succinct with High Latency	More Comm. but with expected Low Latency	
Communication			
[CW89], [BGP92] + [Che21]	$O(nL + n^2 \log n)$	$O(n^2 L) + \mathsf{E}(\text{poly}(n))$	[FM88]
		$O(n^2 L) + \mathsf{E}(O(n^6 \log n))$	[KK06]
		$O(nL) + \mathsf{E}(O(n^4 \log n))$	[AAPP22]
Rounds			
	$\Omega(n)$	$\mathsf{E}(O(1))$	

State of the Art: Broadcast

Succinct with High Latency	More Comm. but with expected Low Latency
Communication	
$O(nL + n^2 \log n)$	$O(n^2L) + \mathrm{E}(\mathrm{poly}(n))$
	$O(n^2L) + \mathrm{E}(O(n^6 \log n))$
	$O(nL) + \mathrm{E}(O(n^4 \log n))$
Rounds	
$\Omega(n)$	$\mathrm{E}(O(1))$

$L = 1$
$n = 300$

$L = 1$
$n = 300$

State of the Art: Broadcast

Succinct with High Latency	More Comm. but with expected Low Latency

Communication

	$O(n^2 L) + \mathrm{E}(\mathrm{poly}(n))$
$O(nL + n^2 \log n)$	$O(n^2 L) + \mathrm{E}(O(n^6 \log n$
	$O(nL) + \mathrm{E}(O(n^4 \log n))$

$L = 1$
$n = 300$
$n^2 \approx 11\mathrm{KB}$

$L = 1$
$n = 300$

Rounds

$\Omega(n)$	$\mathrm{E}(O(1))$

State of the Art: Broadcast

Succinct with High Latency	More Comm. but with expected Low Latency
Communication	
	$O(n^2L) + \mathsf{E}(\text{poly}(n))$
$O(nL + n^2 \log n)$	$O(n^2L) + \mathsf{E}(O(n^6 \log n$
	$O(nL) + \mathsf{E}(O(n^4 \log n))$
Rounds	
$\Omega(n)$	$\mathsf{E}(O(1))$

$L = 1$
$n = 300$
$n^2 \approx 11\text{KB}$

$L = 1$
$n = 300$
$n^4 \approx 1\text{GB}$

State of the Art: Broadcast

Succinct with High Latency

More Comm. but with expected Low Latency

Communication

$O(n^2L) + \mathsf{E}(\mathrm{poly}(n))$

$O(nL + n^2 \log n)$

$O(n^2L) + \mathsf{E}(O(n^6 \log n))$

$O(nL) + \mathsf{E}(O(n^4 \log n))$

Rounds

$\Omega(n)$

$\mathsf{E}(O(1))$

$L = 1$
$n = 300$
$n^2 \approx 11\text{KB}$

$L = 1$
$n = 300$
$n^4 \approx 1\text{GB}$

10 round protocol
$O(3000)$ rounds

10 round protocol
Expected $O(10)$ rounds

Succinct Broadcast with Expected Low Latency?

Our Results #1: Broadcast

	Succinct with High Latency	**More Comm. but with expected Low Latency**	
Communication	[CW89], [BGP92] + [Che21]	[AAPP22]	
	$O(nL + n^2 \log n)$	$O(nL) + \mathsf{E}(O(n^4 \log n))$	
		$O(nL + n^2)$	Best we can hope for
Rounds	$\Omega(n)$	$\mathsf{E}(O(1))$	

Our Results #1: Broadcast

	Succinct with High Latency	**More Comm. but with expected Low Latency**	
Communication			
[CW89], [BGP92] + [Che21]	$O(nL + n^2 \log n)$	$O(nL) + \mathsf{E}(O(n^4 \log n))$	[AAPP22]
		$O(nL + n^2)$	Best we can hope for
		$O(nL) + \mathsf{E}(O(n^3 \log^2 n))$	This work
Rounds	$\Omega(n)$	$\mathsf{E}(O(1))$	

Broadcast for MPC

- Secure computation protocols assume broadcast
- [BGW88] Verifiable Secret Sharing:
  - Complain about the dealer
  - Vote on the dealer

Broadcast for MPC

- Secure computation protocols assume broadcast
- [BGW88] Verifiable Secret Sharing:
  - Complain about the dealer
  - Vote on the dealer

Communication Pattern

Broadcast for MPC

- Secure computation protocols assume broadcast
- [BGW88] Verifiable Secret Sharing:
  - Complain about the dealer
  - Vote on the dealer

Communication Pattern

$1 \times \mathsf{BC}(L)$

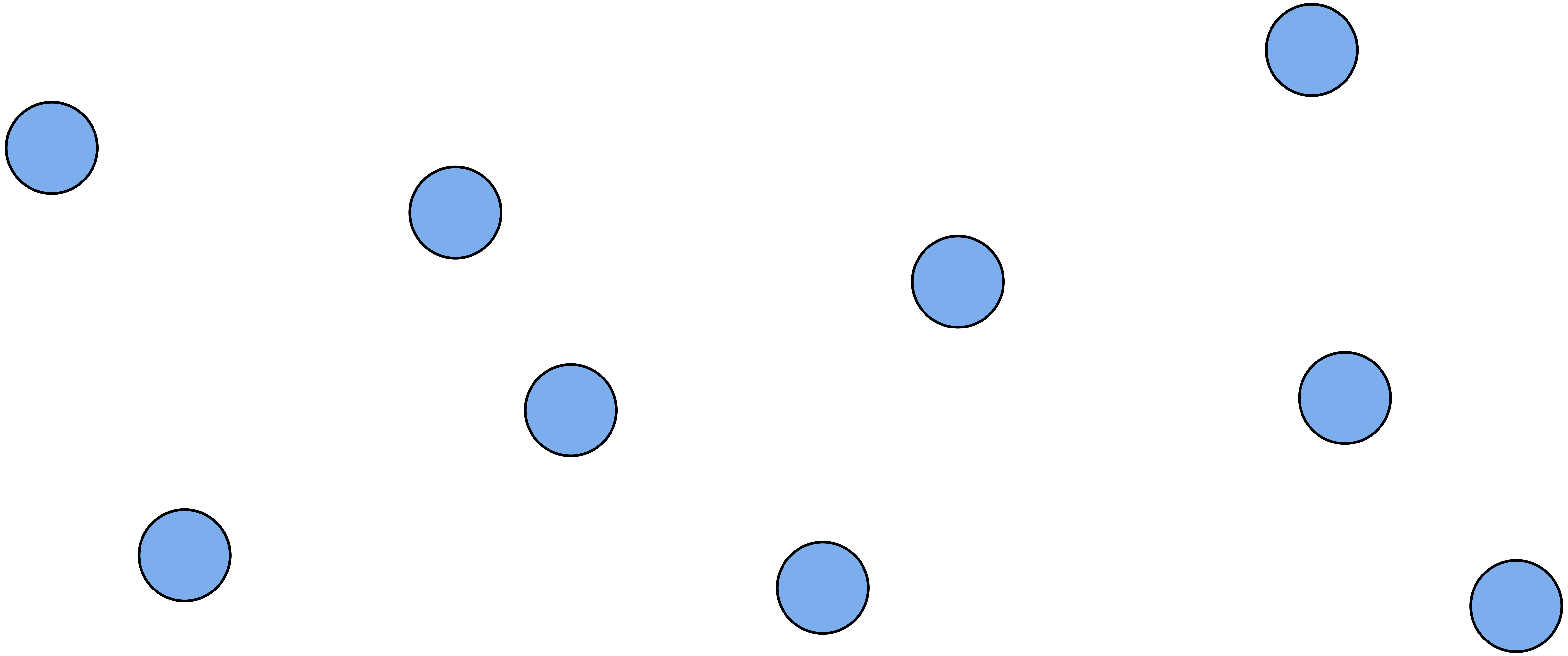
Broadcast for MPC

- Secure computation protocols assume broadcast
- [BGW88] Verifiable Secret Sharing:
  - Complain about the dealer
  - Vote on the dealer

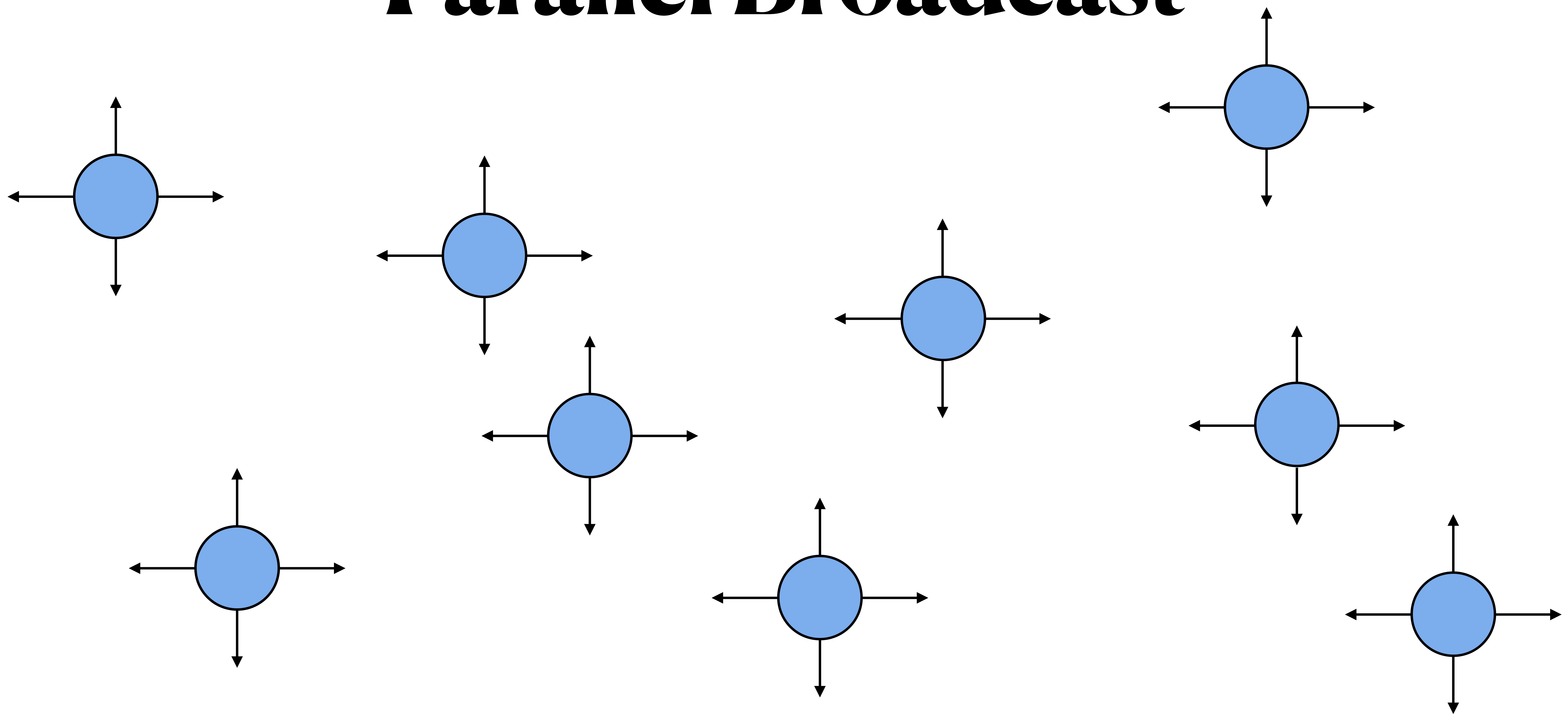
Communication Pattern

$1 \times \mathsf{BC}(L)$ $\quad$ $n \times \mathsf{BC}(L)$

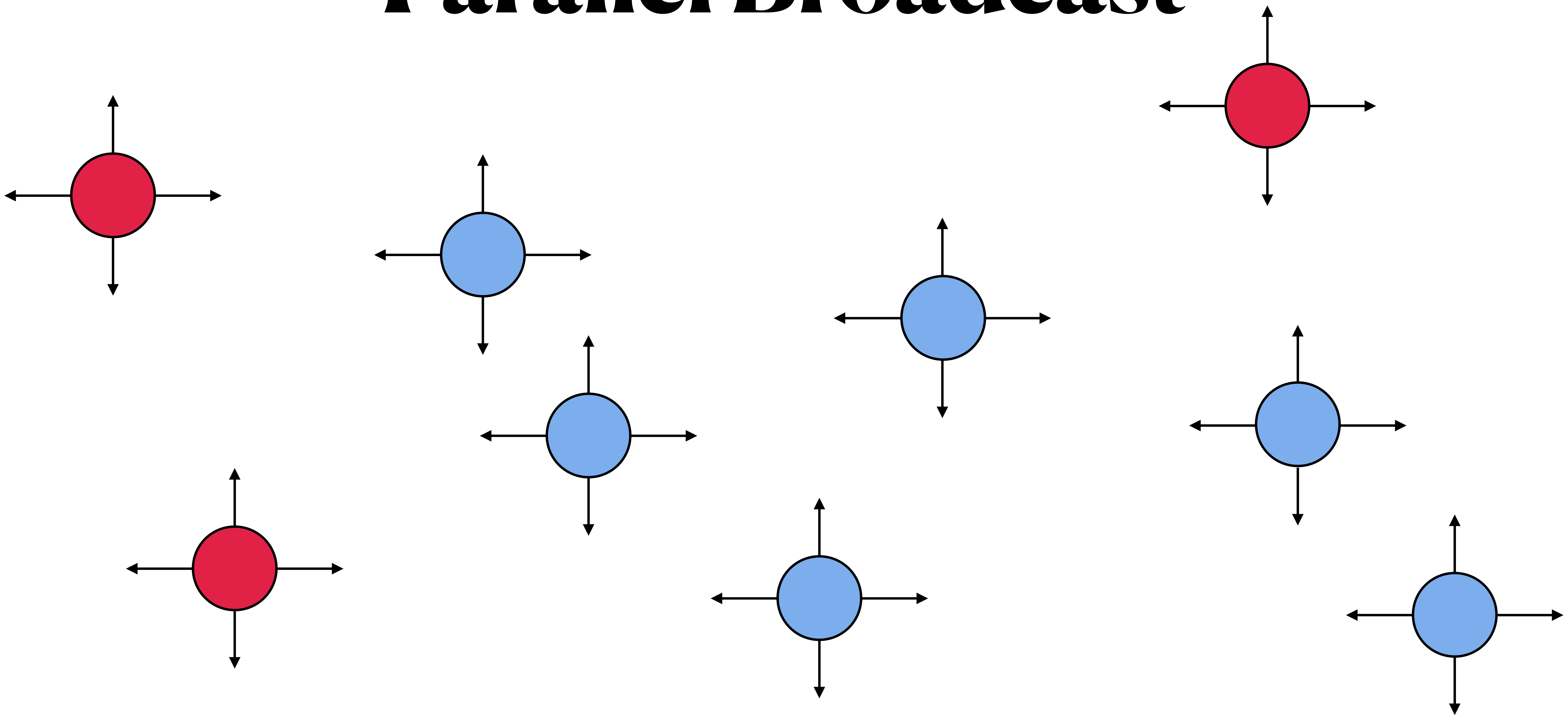
Parallel Broadcast



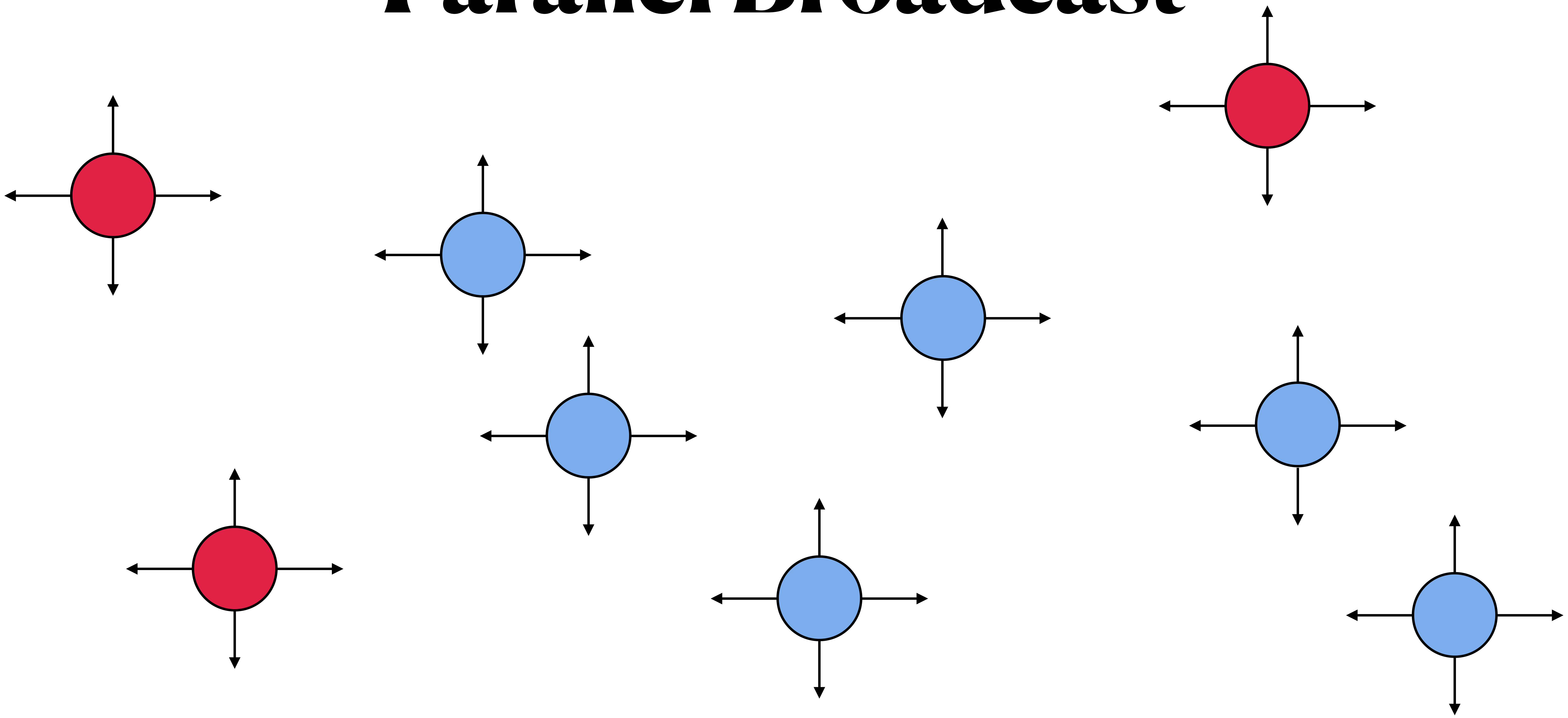
Parallel Broadcast



Parallel Broadcast



Parallel Broadcast



- **Agreement:** On the messages of all senders
- **Validity:** Output each honest sender's message

State of the Art: Parallel Broadcast

State of the Art: Parallel Broadcast

Succinct with High Latency

State of the Art: Parallel Broadcast

Succinct with High Latency

More Comm. but with expected Low Latency

State of the Art: Parallel Broadcast

Succinct with High Latency

More Comm. but with expected Low Latency

Communication

Rounds

State of the Art: Parallel Broadcast

Succinct with High Latency

More Comm. but with expected Low Latency

Communication

$O(n^2L + n^3 \log n)$

Rounds

$\Omega(n)$

State of the Art: Parallel Broadcast

Succinct with High Latency

More Comm. but with expected Low Latency

Communication

[CW89], [BGP92] + [Che21]

$O(n^2L + n^3 \log n)$

Rounds

$\Omega(n)$

State of the Art: Parallel Broadcast

Succinct with High Latency	More Comm. but with expected Low Latency

[CW89], [BGP92] + [Che21]

Communication

$O(n^2 L + n^3 \log n)$

$O(n^2 L) + \mathrm{E}(\mathrm{poly}(n))$

Rounds

$\Omega(n)$

State of the Art: Parallel Broadcast

Succinct with High Latency	More Comm. but with expected Low Latency
[CW89], [BGP92] + [Che21]	[FG03] [FM88]
Communication: $O(n^2L + n^3 \log n)$	**Communication:** $O(n^2L) + \mathrm{E}(\mathrm{poly}(n))$
Rounds: $\Omega(n)$	**Rounds:** $\mathrm{E}(O(1))$

State of the Art: Parallel Broadcast

	Succinct with High Latency	**More Comm. but with expected Low Latency**	
			[FG03]
Communication		$O(n^2L) + \mathsf{E}(\text{poly}(n))$	[FM88]
[CW89], [BGP92] + [Che21]	$O(n^2L + n^3 \log n)$	$O(n^2L) + \mathsf{E}(O(n^6 \log n))$	[KK06]
Rounds	$\Omega(n)$	$\mathsf{E}(O(1))$	

State of the Art: Parallel Broadcast

Succinct with High Latency		More Comm. but with expected Low Latency	[FG03]
Communication			
[CW89], [BGP92] + [Che21]	$O(n^2L + n^3 \log n)$	$O(n^2L) + \mathsf{E}(\mathrm{poly}(n))$	[FM88]
		$O(n^2L) + \mathsf{E}(O(n^6 \log n))$	[KK06]
		$O(n^2L) + \mathsf{E}(O(n^4 \log n))$	[AAPP22]
Rounds			
	$\Omega(n)$	$\mathsf{E}(O(1))$	

State of the Art: Parallel Broadcast

	Succinct with High Latency	More Comm. but with expected Low Latency	
Communication			[FG03]
		$O(n^2L) + \mathrm{E}(\mathrm{poly}(n))$	[FM88]
[CW89], [BGP92] + [Che21]	$O(n^2L + n^3 \log n)$	$O(n^2L) + \mathrm{E}(O(n^6 \log n))$	[KK06]
		$O(n^2L) + \mathrm{E}(O(n^4 \log n))$	[AAPP22]
Rounds	$\Omega(n)$	$\mathrm{E}(O(1))$	

Succinct (Parallel) Broadcast with Expected Low Latency?

Our Results #2: Parallel Broadcast

	Succinct with High Latency	More Comm. but with expected Low Latency	[FG03]
[CW89], [BGP92] + [Che21]			
Communication	$O(n^2L + n^3 \log n)$	$O(n^2L) + \mathrm{E}(O(n^4 \log n))$	[AAPP22]
		$O(n^2L)$	Best we can hope for
Rounds	$\Omega(n)$	$\mathrm{E}(O(1))$	

Our Results #2: Parallel Broadcast

	Succinct with High Latency	More Comm. but with expected Low Latency	
Communication			
[CW89], [BGP92] + [Che21]	$O(n^2L + n^3 \log n)$	$O(n^2L) + \mathsf{E}(O(n^4 \log n))$	[FG03] [AAPP22]
		$O(n^2L)$	Best we can hope for
		$O(n^2L) + \mathsf{E}(O(n^3 \log^2 n))$	This work
Rounds	$\Omega(n)$	$\mathsf{E}(O(1))$	

Our Results #2: Parallel Broadcast

	Succinct with High Latency	**More Comm. but with expected Low Latency**	
			[FG03]
Communication			
[CW89], [BGP92] + [Che21]	$O(n^2L + n^3 \log n)$	$O(n^2L) + \mathsf{E}(O(n^4 \log n))$	[AAPP22]
		$O(n^2L)$	Best we can hope for
		$O(n^2L) + \mathsf{E}(O(n^3 \log^2 n))$	This work
Rounds	$\Omega(n)$	$\mathsf{E}(O(1))$	

Our Results #2: Parallel Broadcast

	Succinct with High Latency	More Comm. but with expected Low Latency	[FG03]
Communication			
[CW89], [BGP92] + [Che21]	$O(n^2L + n^3 \log n)$	$O(n^2L) + \mathrm{E}(O(n^4 \log n))$	[AAPP22]
		$O(n^2L)$	Best we can hope for
		$O(n^2L) + \mathrm{E}(O(n^3 \log^2 n))$	This work
Rounds	$\Omega(n)$	$\mathrm{E}(O(1))$	

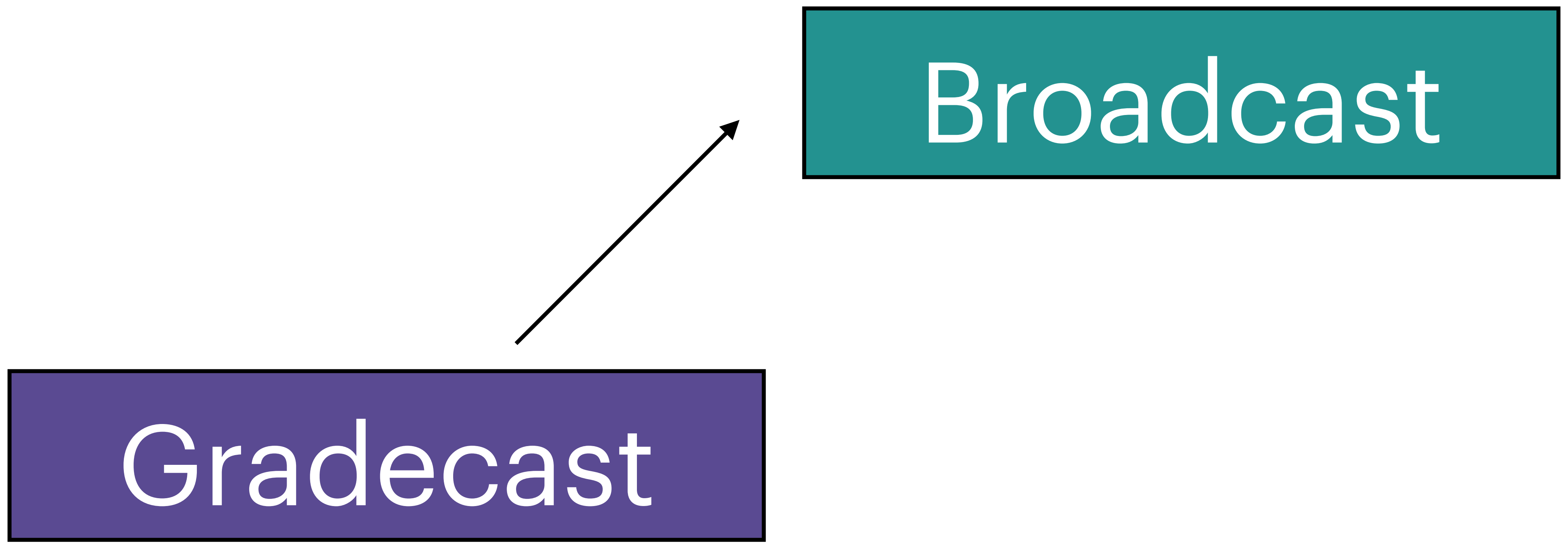
We are optimal for $L \geq n \log^2 n$

Broadcast

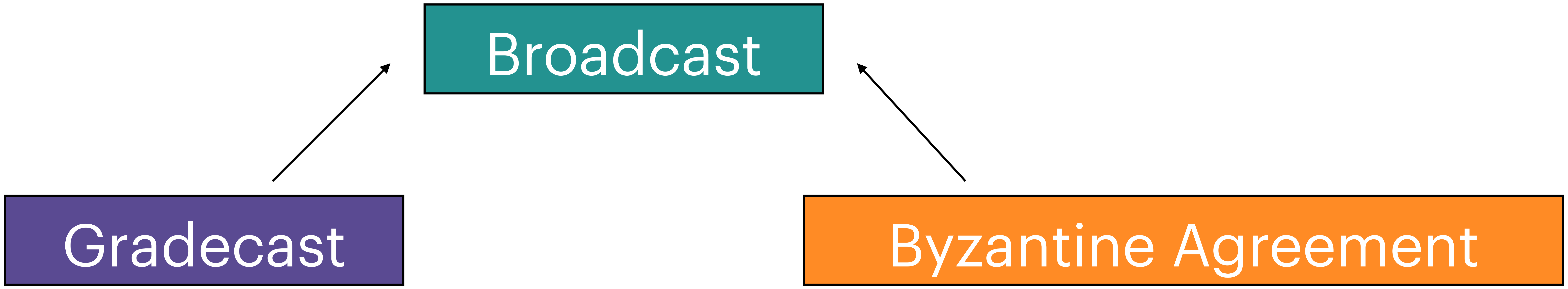
[KK06] Framework

Broadcast

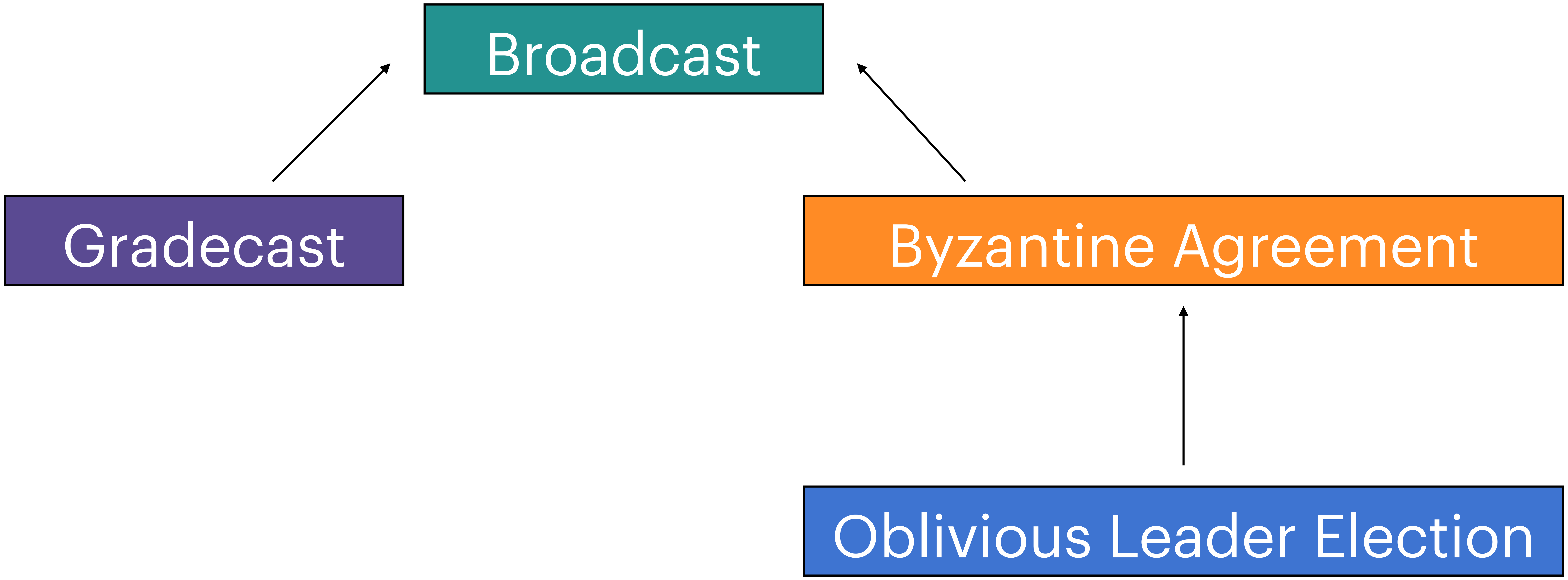
[KK06] Framework



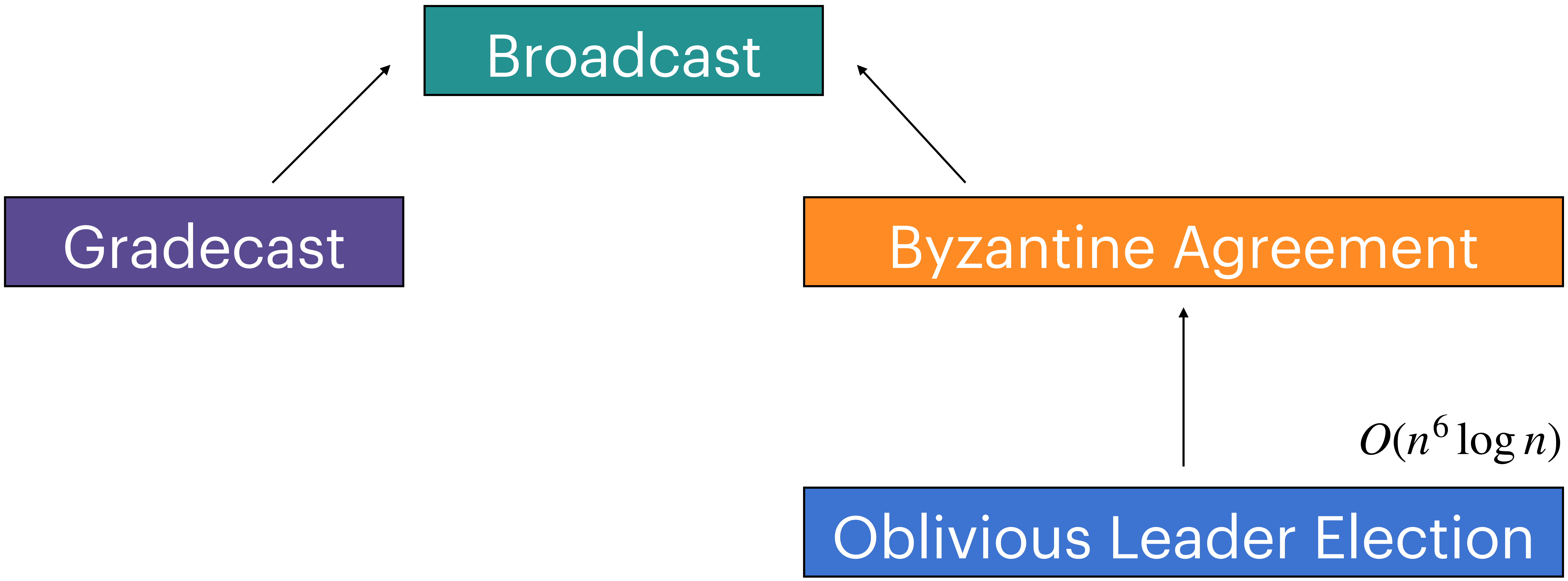
[KK06] Framework



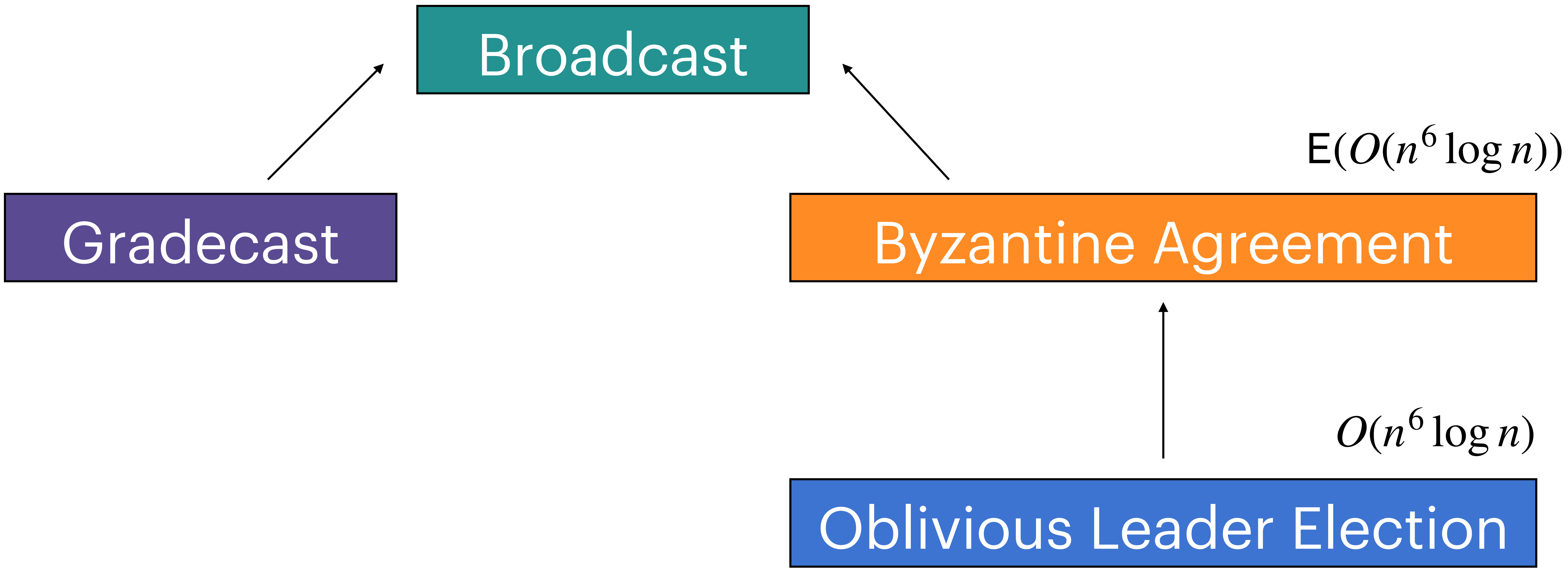
[KK06] Framework



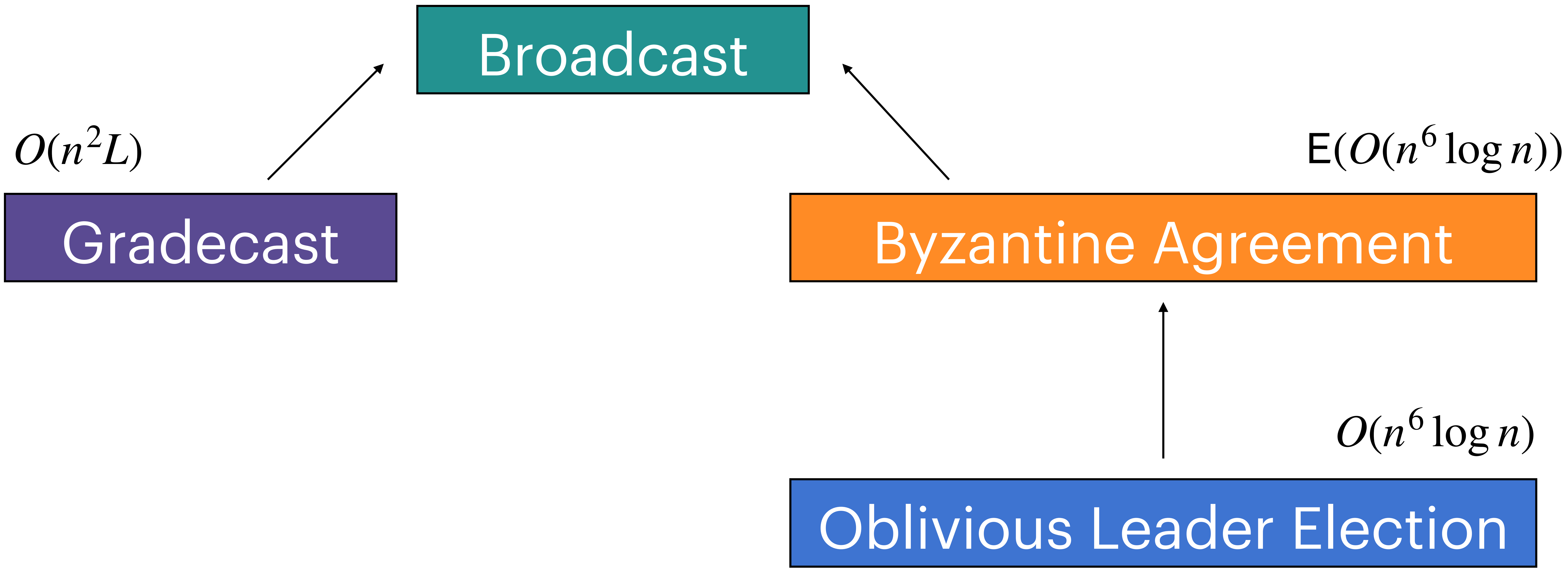
[KK06] Framework



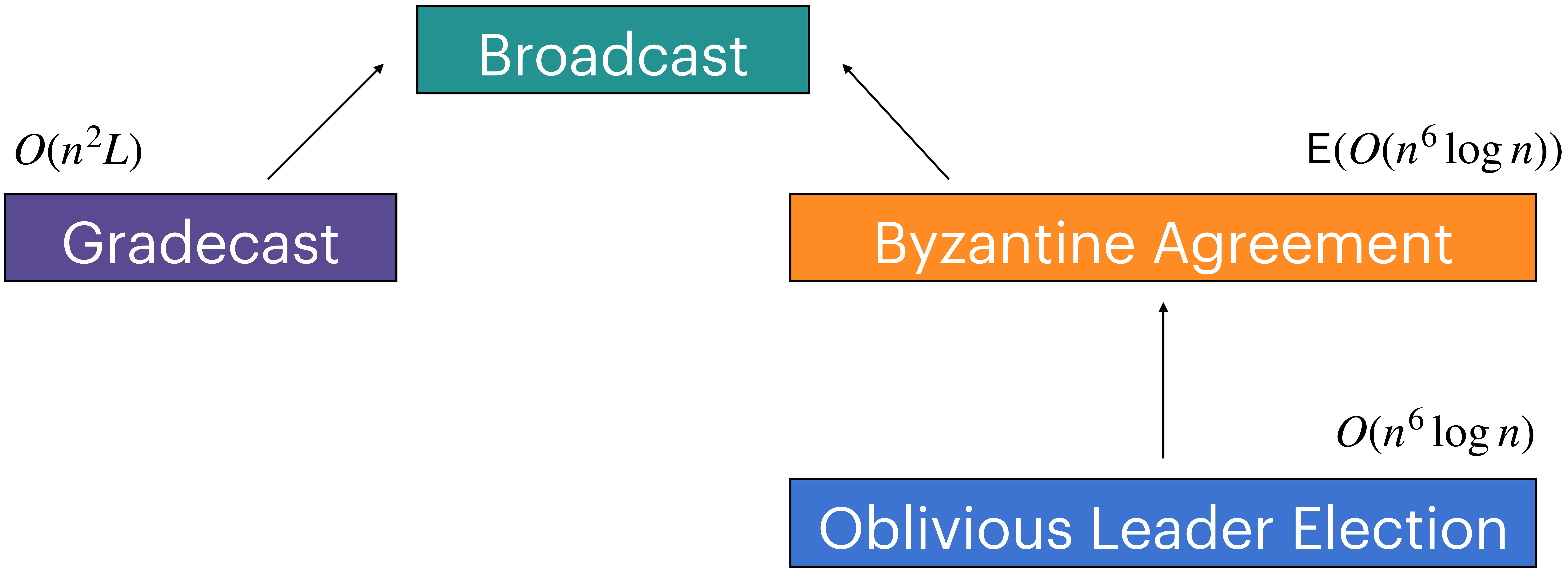
[KK06] Framework



[KK06] Framework

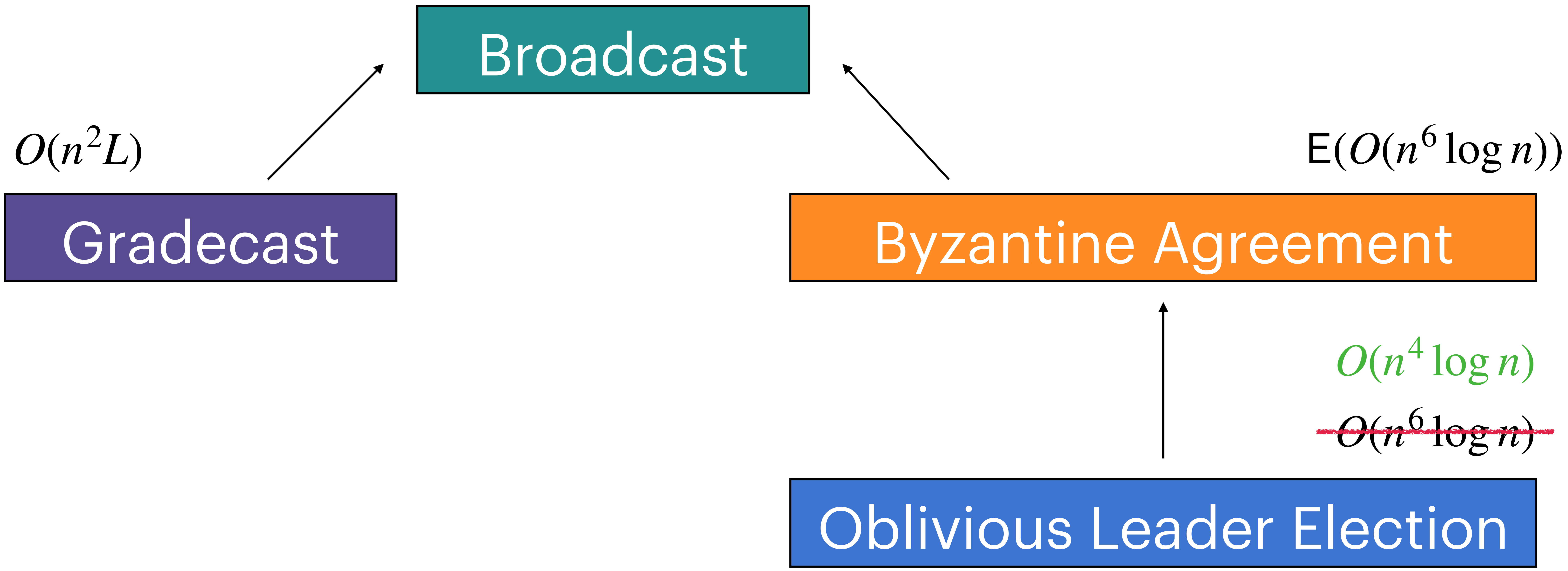


[KK06] Framework



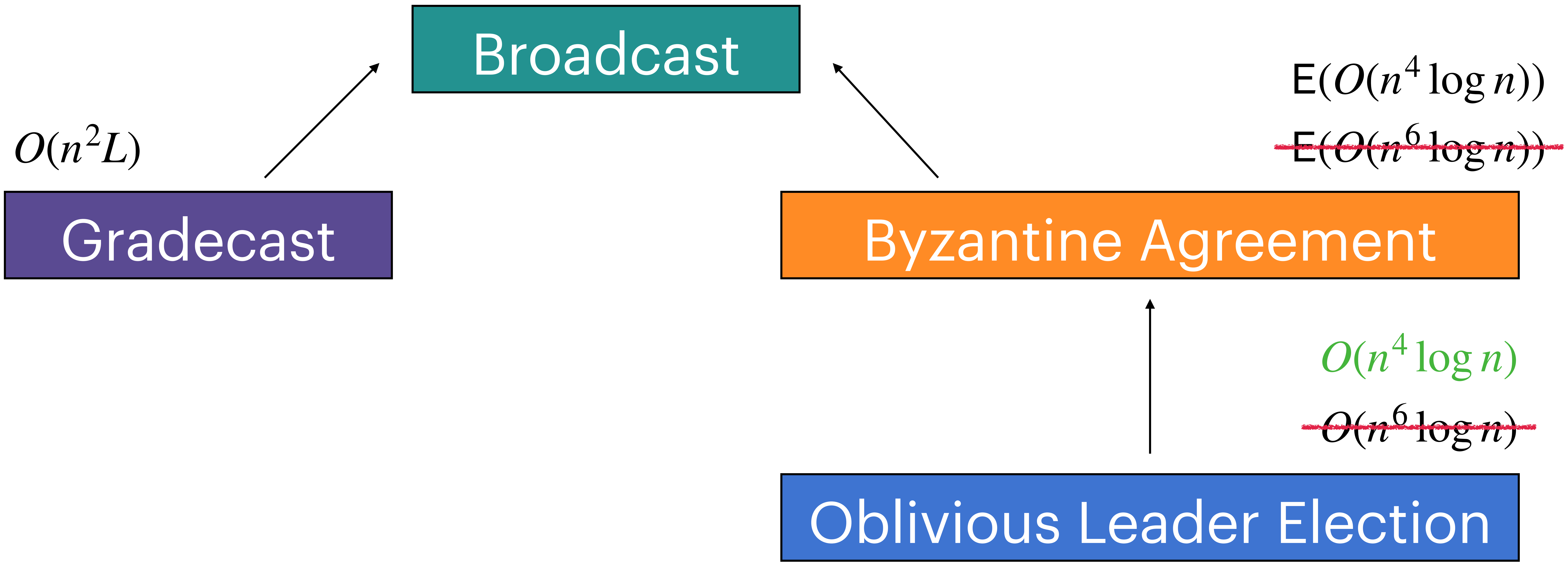
[Abraham, Asharov, Patil, Patra; 22] Improvements

[KK06] Framework



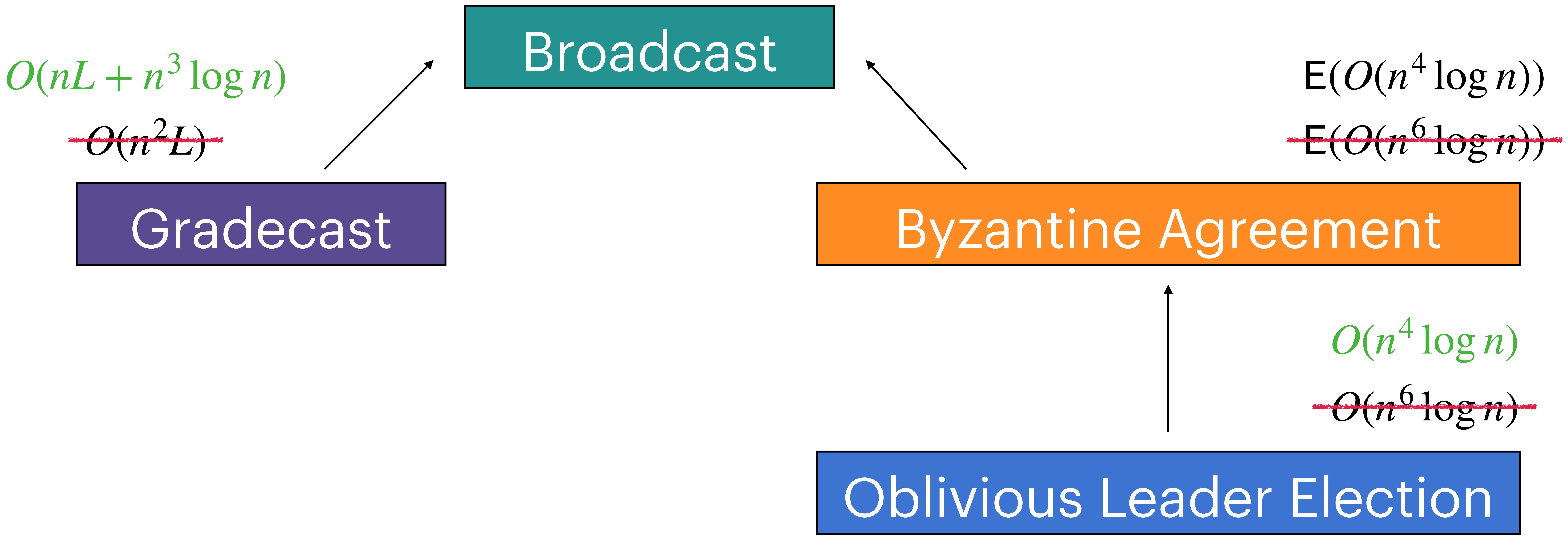
[Abraham, Asharov, Patil, Patra; 22] Improvements

[KK06] Framework



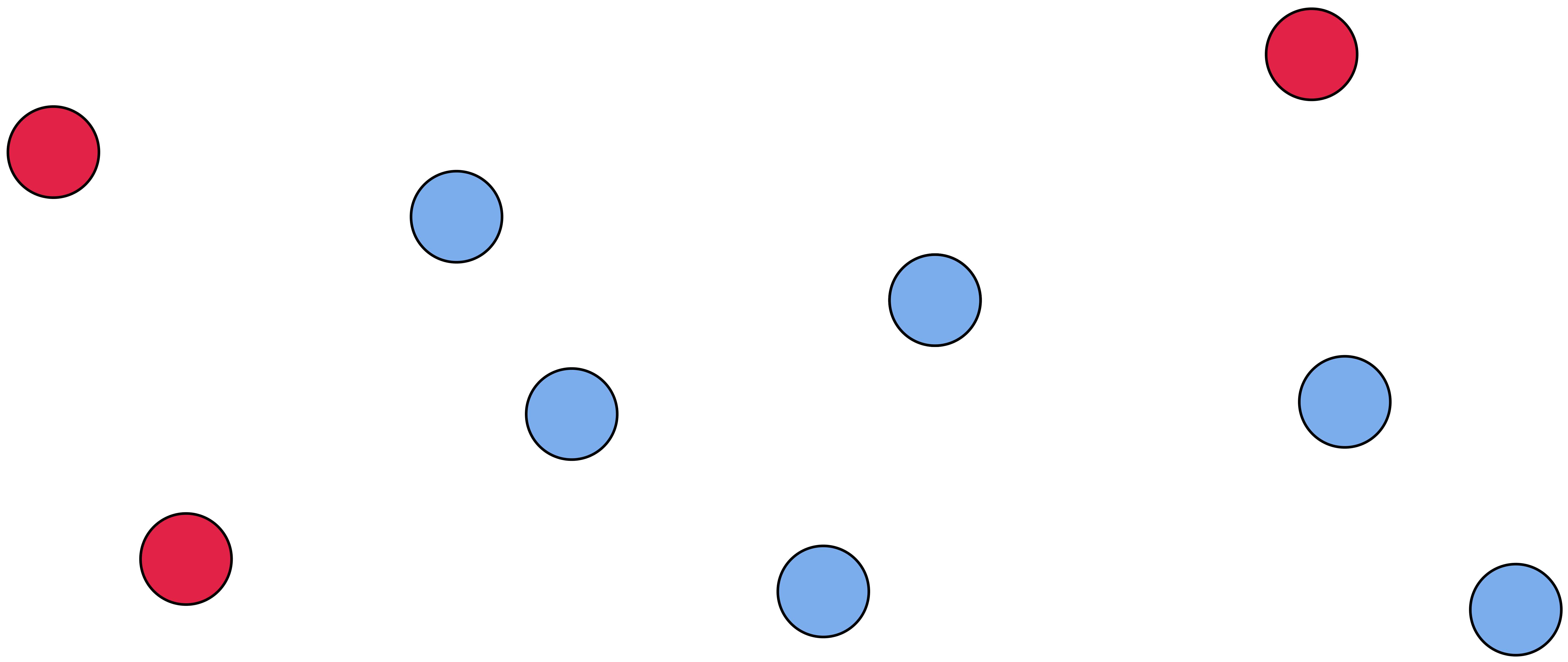
[Abraham, Asharov, Patil, Patra; 22] Improvements

[KK06] Framework

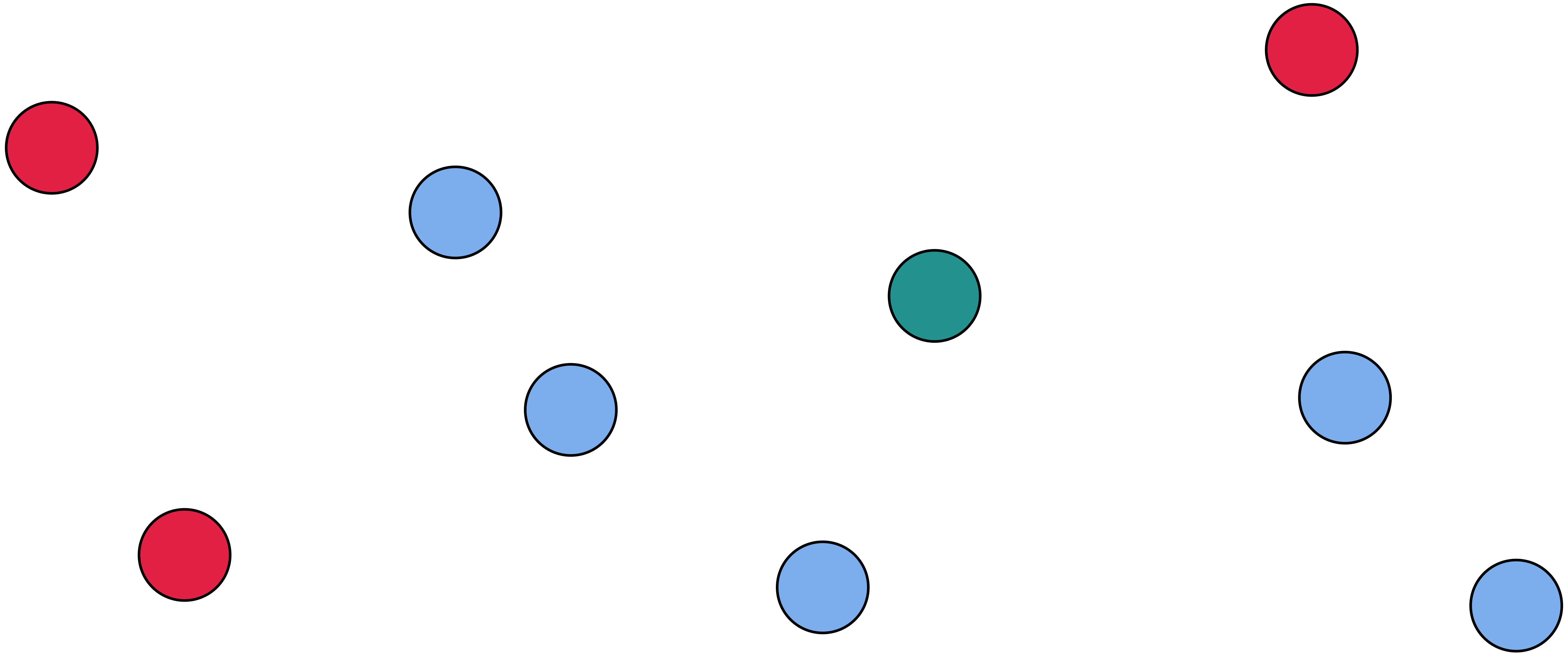


[Abraham, Asharov, Patil, Patra; 22] Improvements

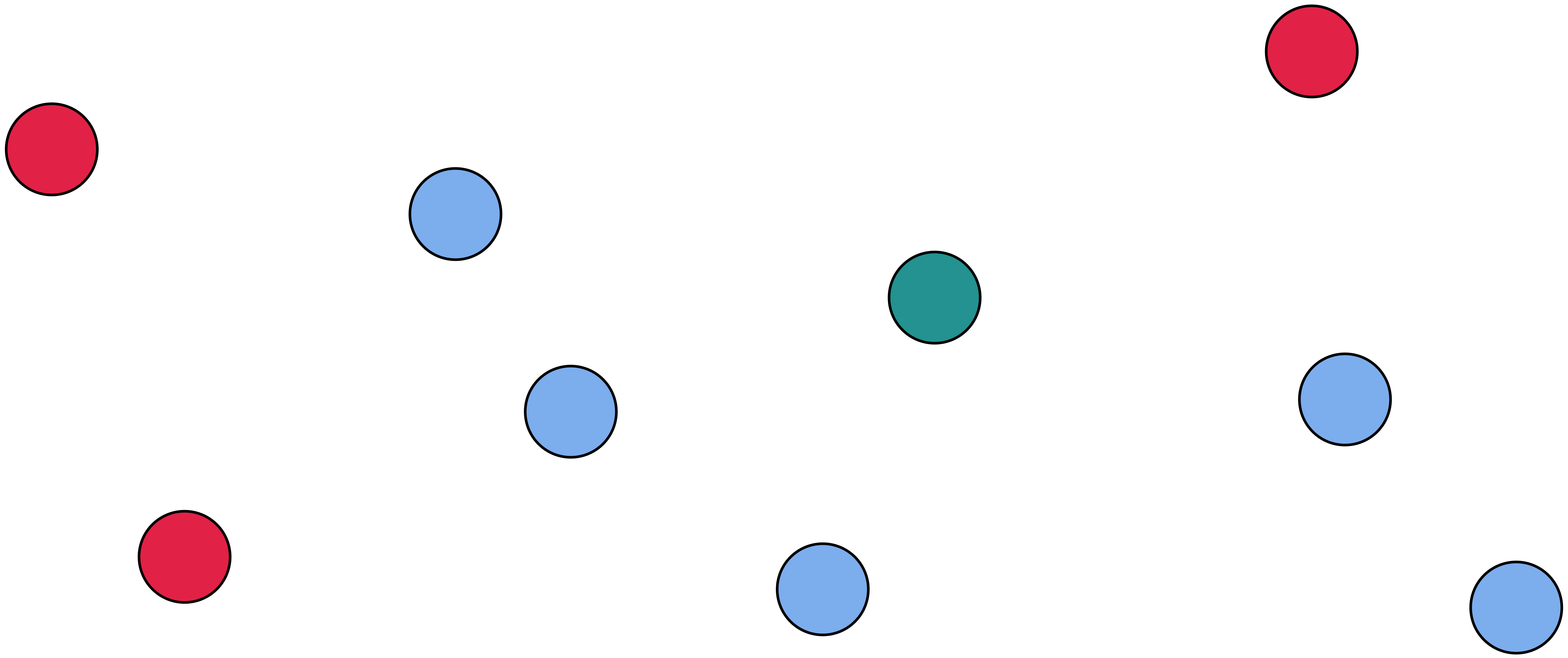
Oblivious Leader Election



Oblivious Leader Election

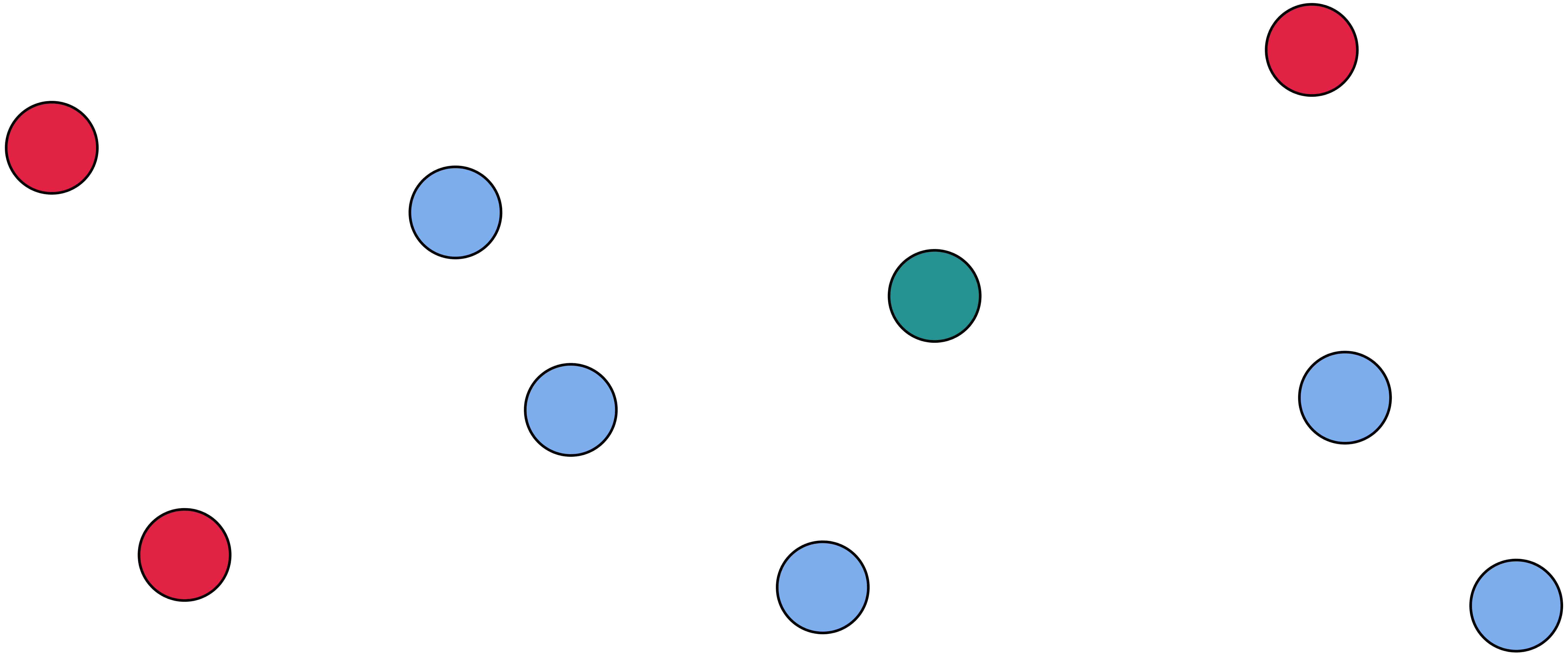


Oblivious Leader Election



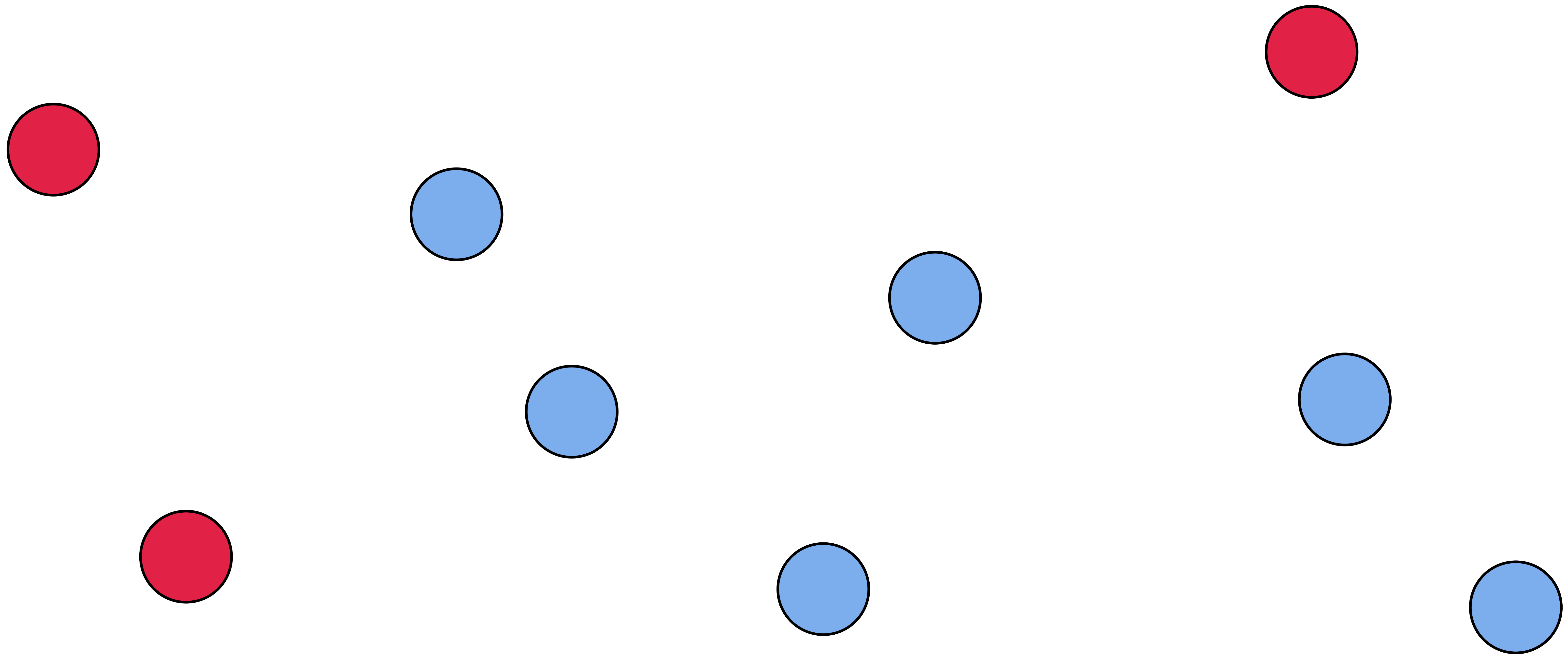
$$\Pr[\text{Everyone agrees on an honest leader}] \geq \frac{1}{2}$$

Oblivious Leader Election

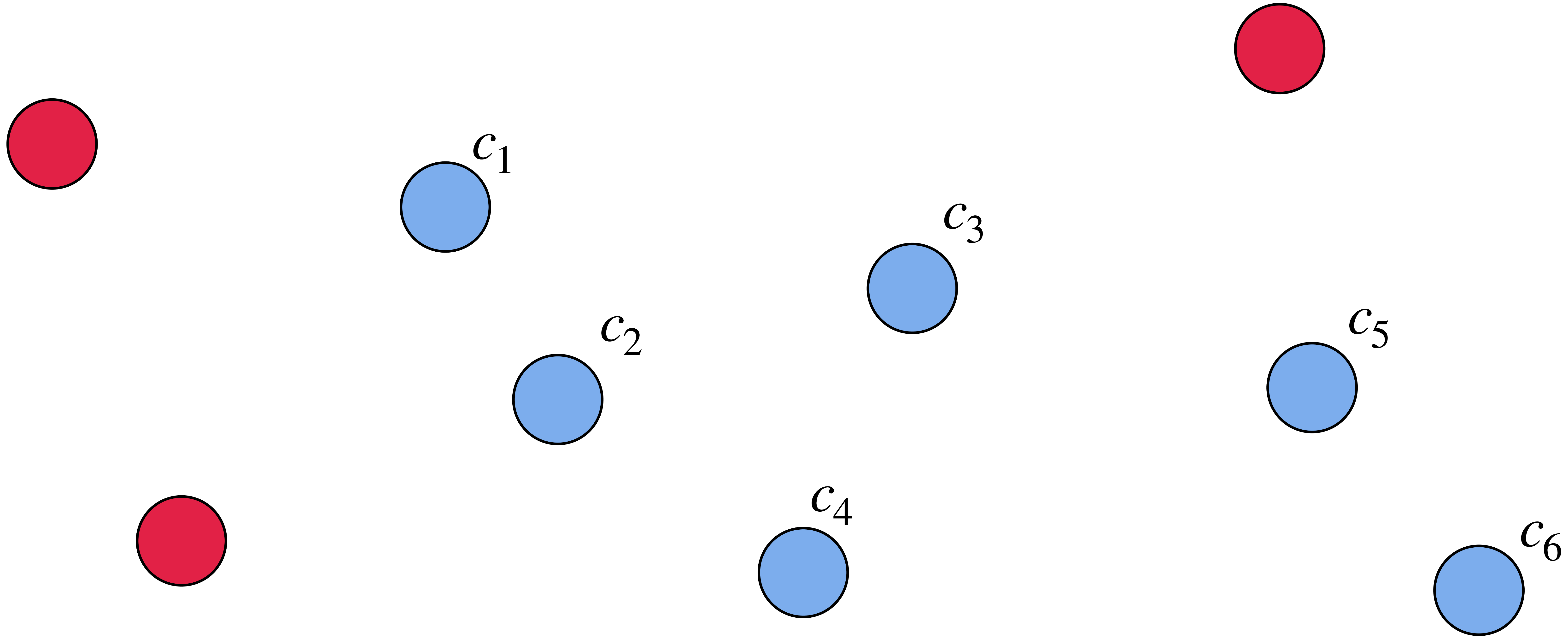


$\Pr[\text{Everyone agrees on an honest leader}] \geq \frac{1}{2}$ Can be any constant!

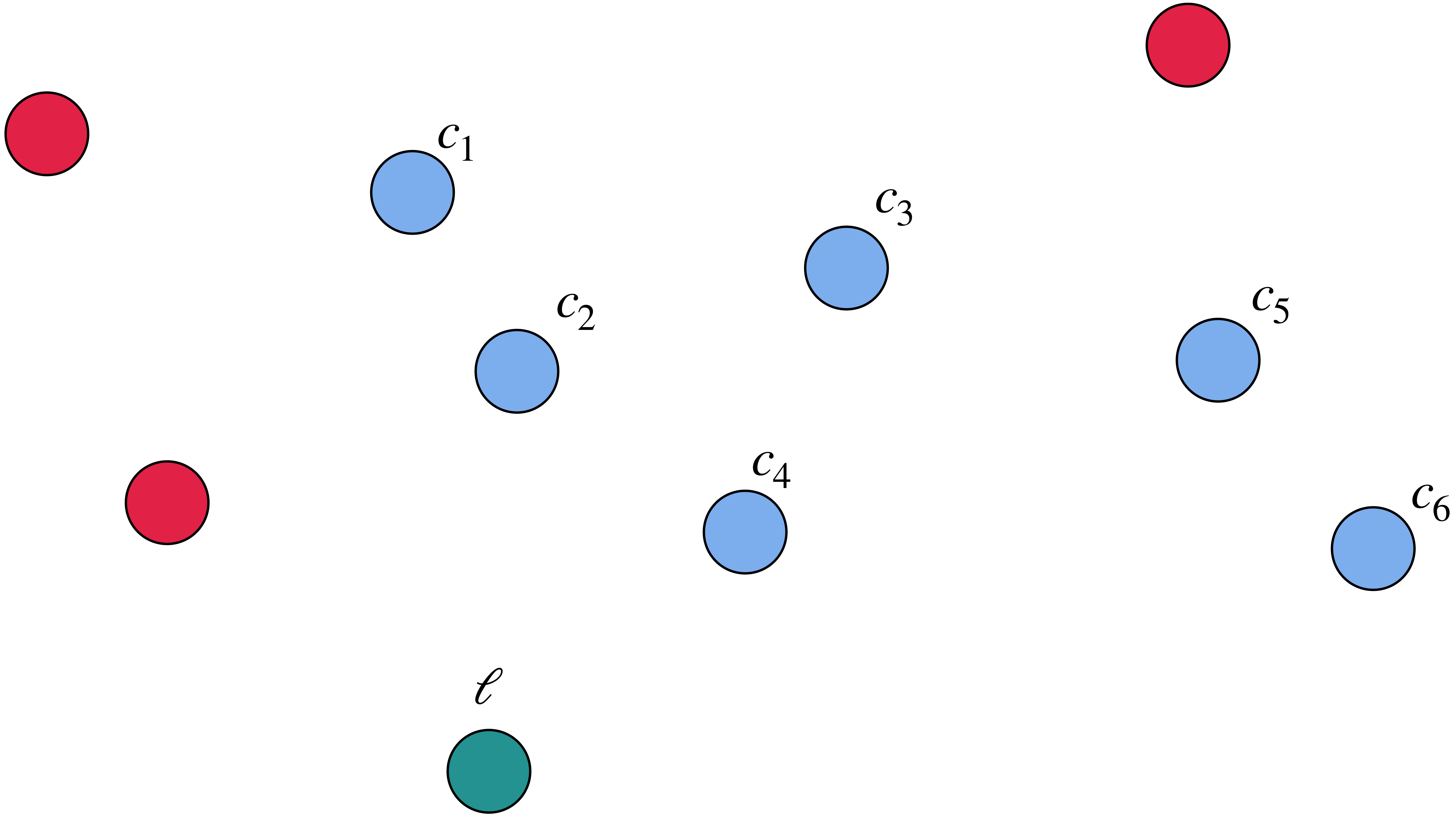
Oblivious Leader Election



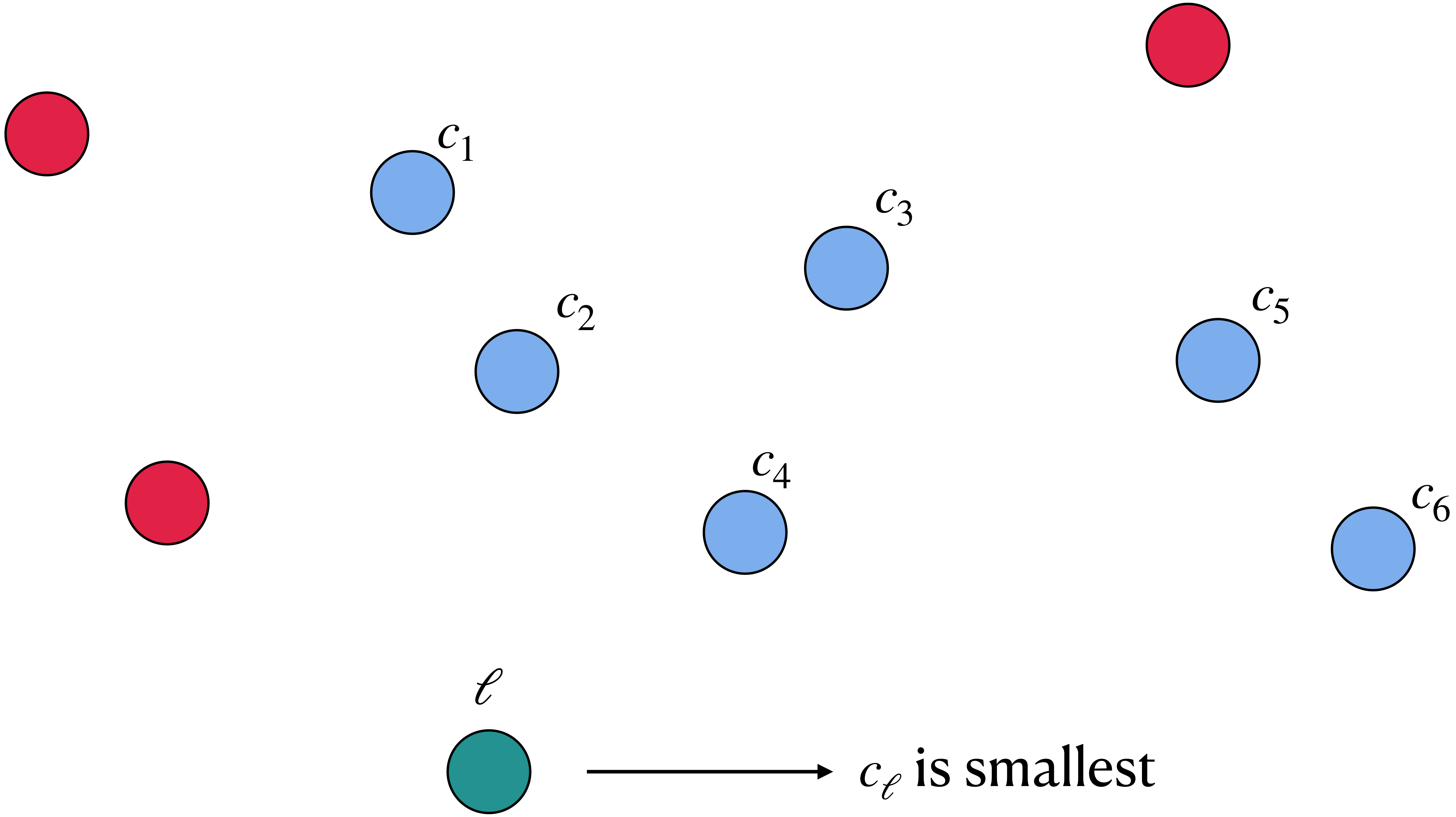
Oblivious Leader Election



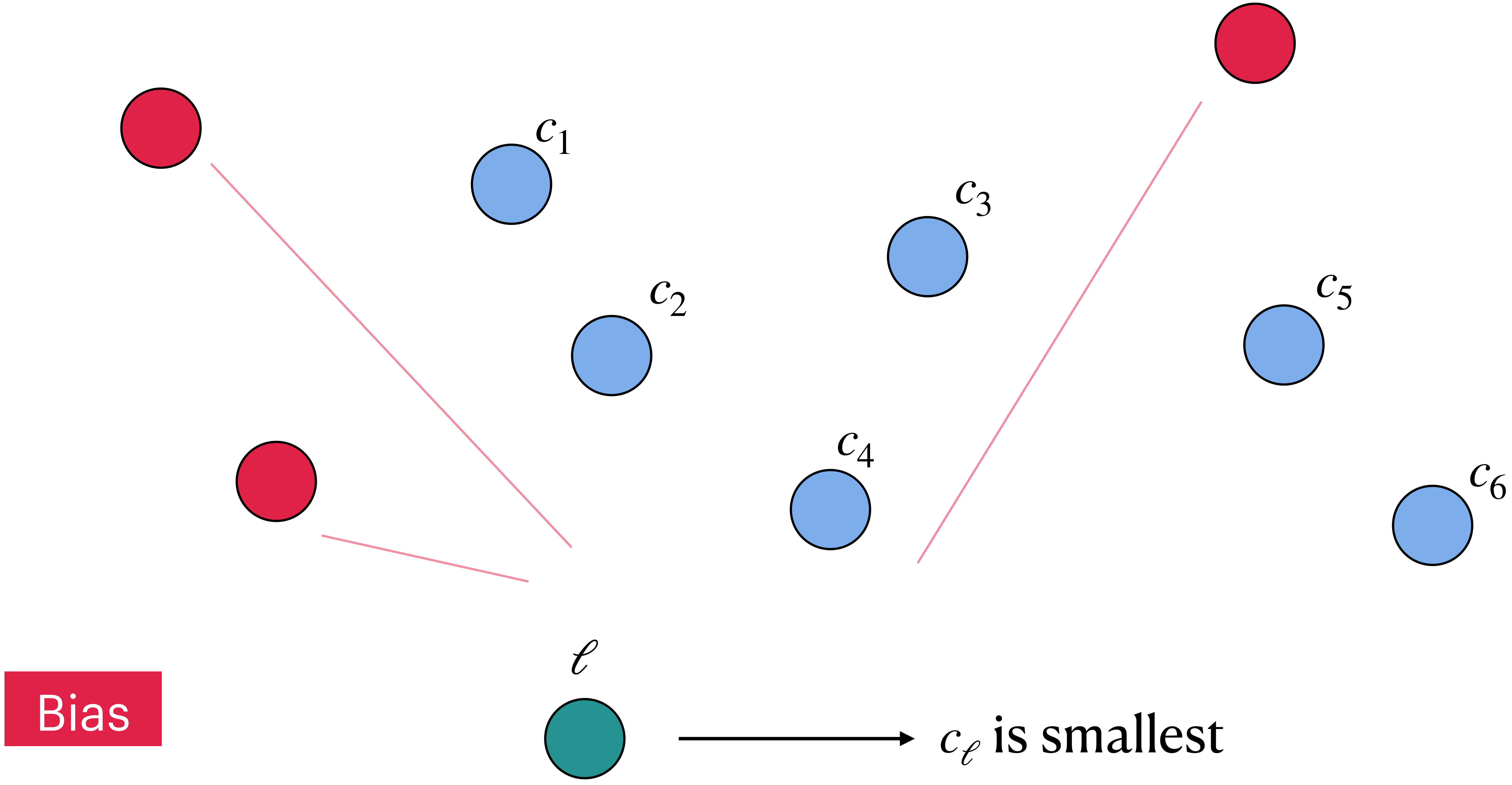
Oblivious Leader Election



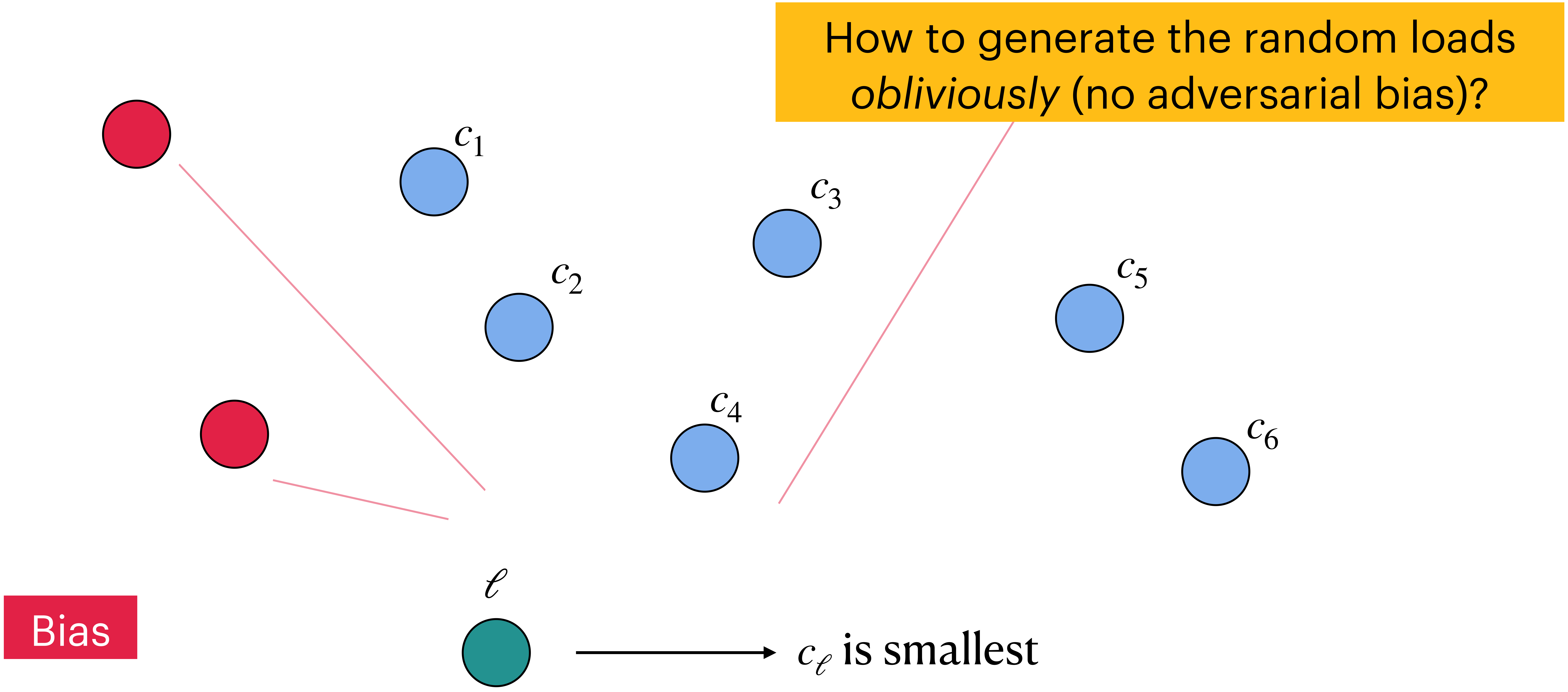
Oblivious Leader Election



Oblivious Leader Election



Oblivious Leader Election

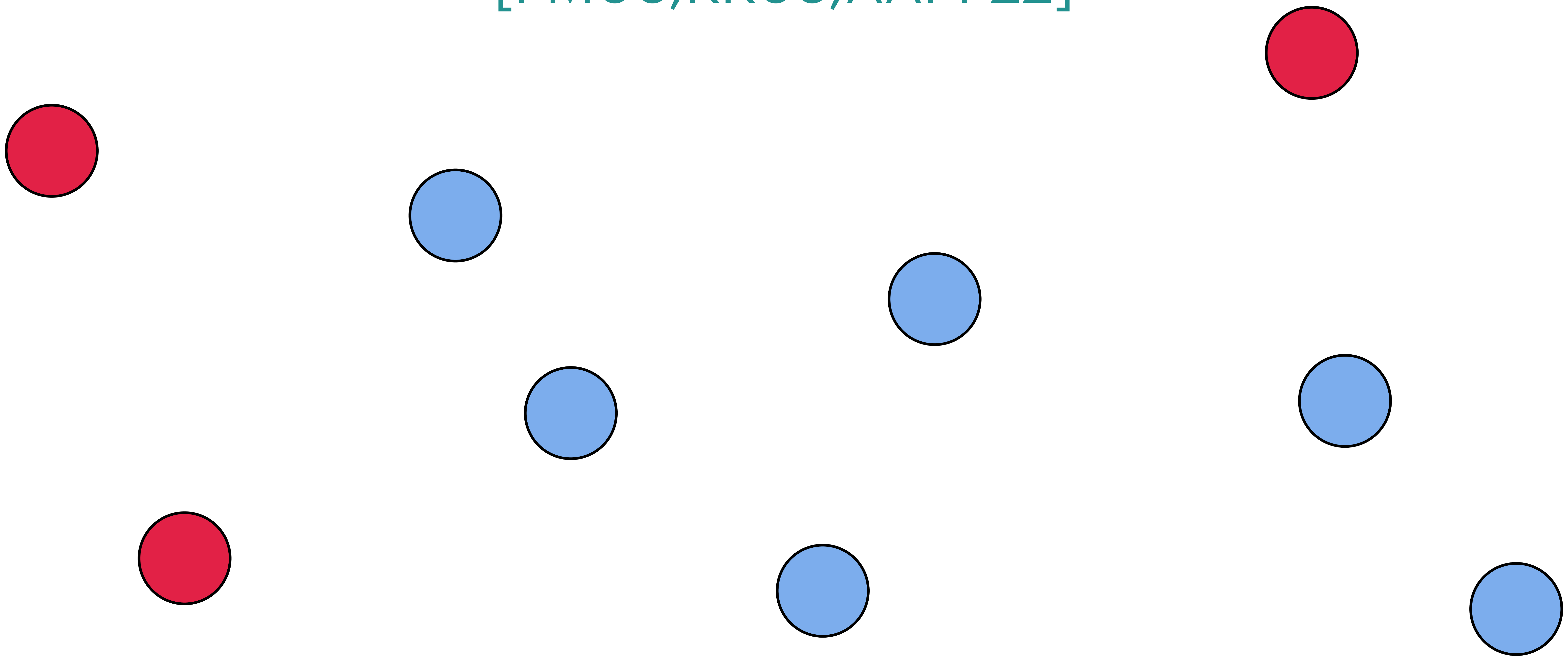


Leader Election from Commitments

[FM06,KK08,AAPP22]

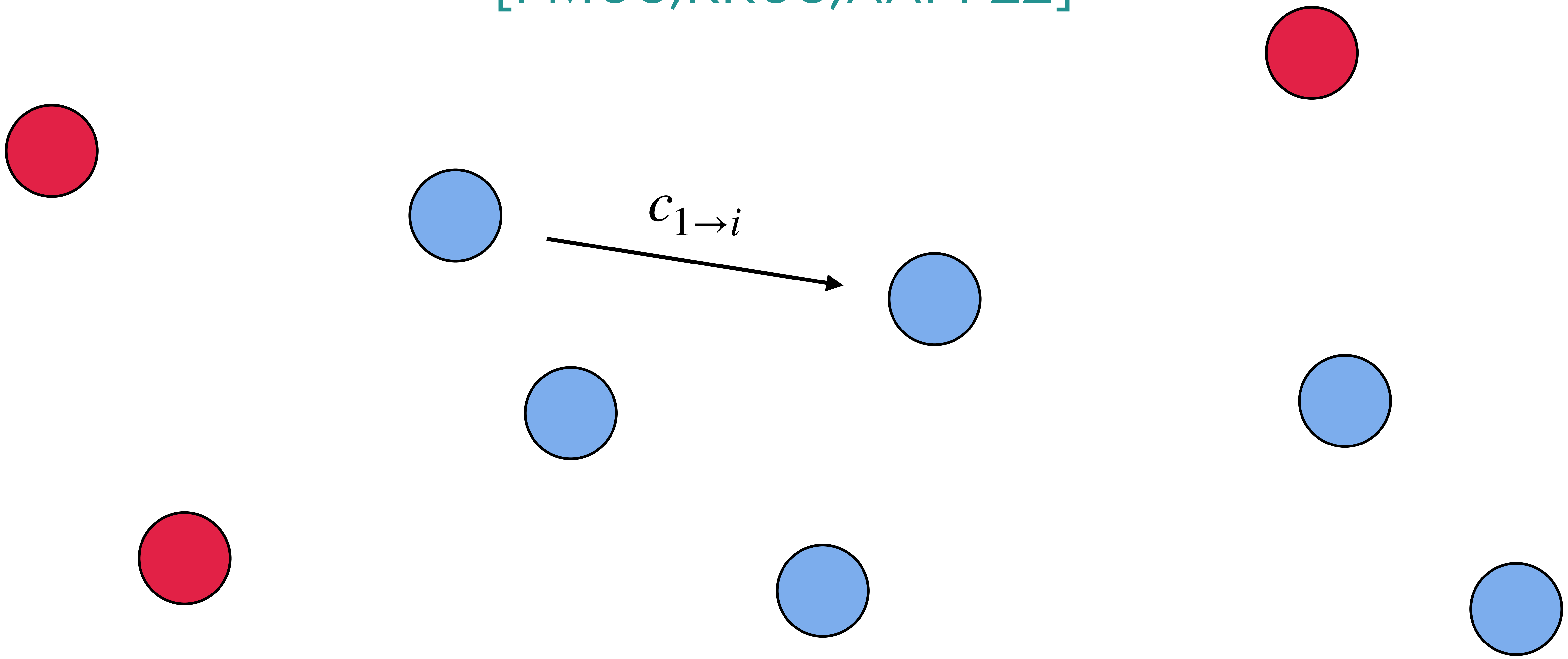
Leader Election from Commitments

[FM06,KK08,AAPP22]



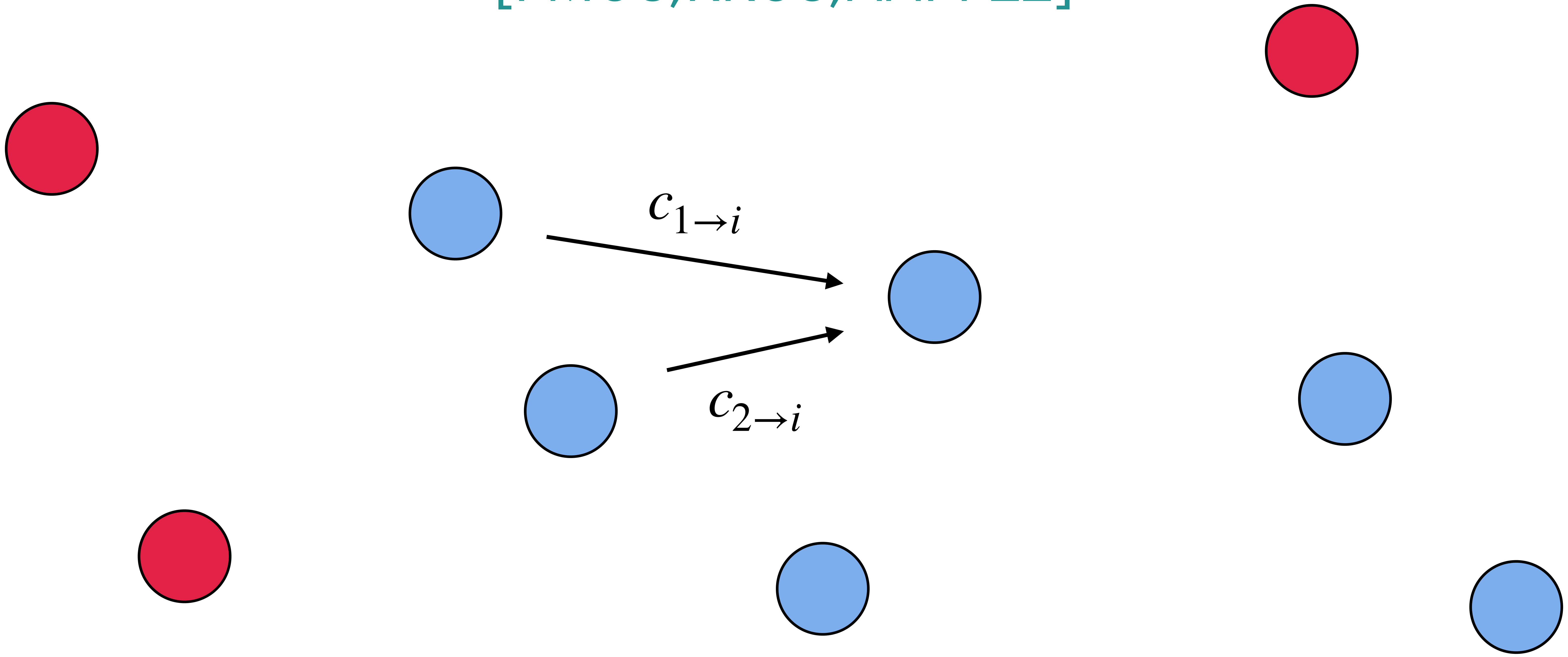
Leader Election from Commitments

[FM06,KK08,AAPP22]



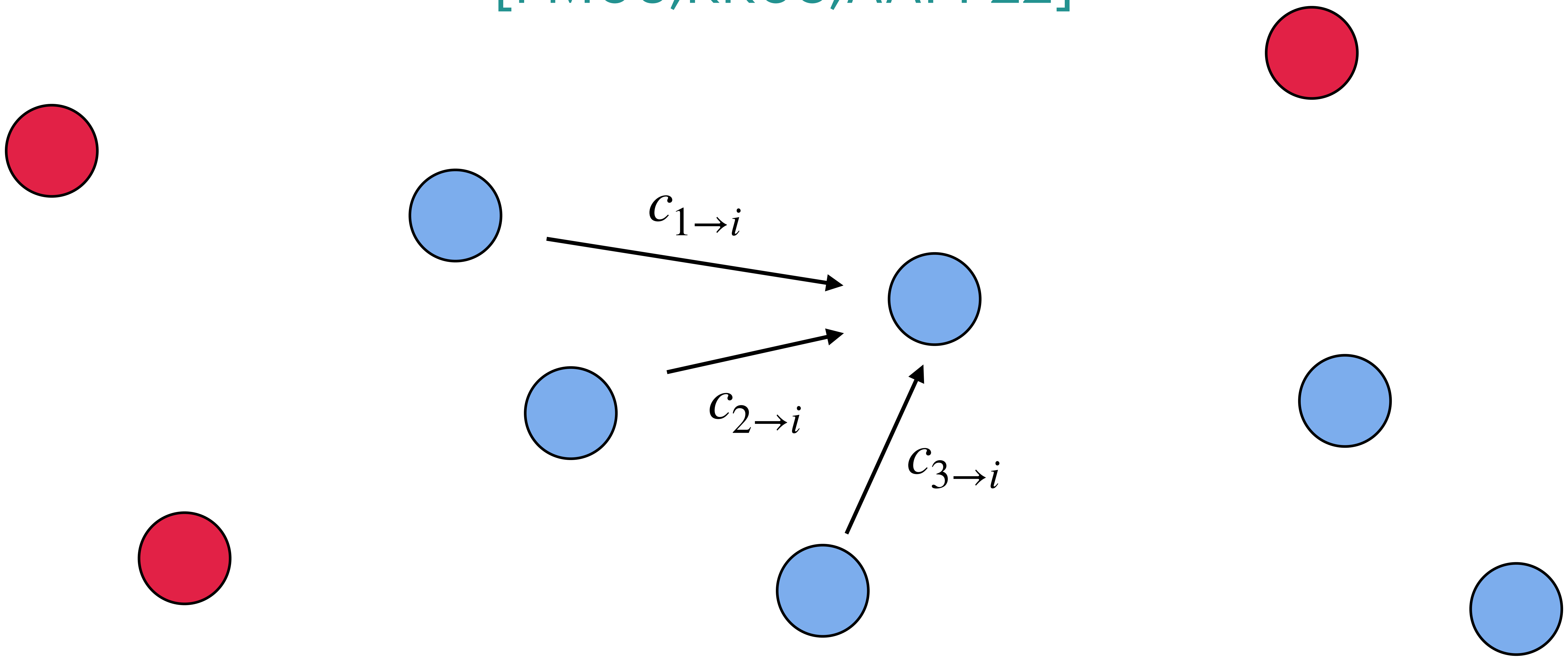
Leader Election from Commitments

[FM06,KK08,AAPP22]



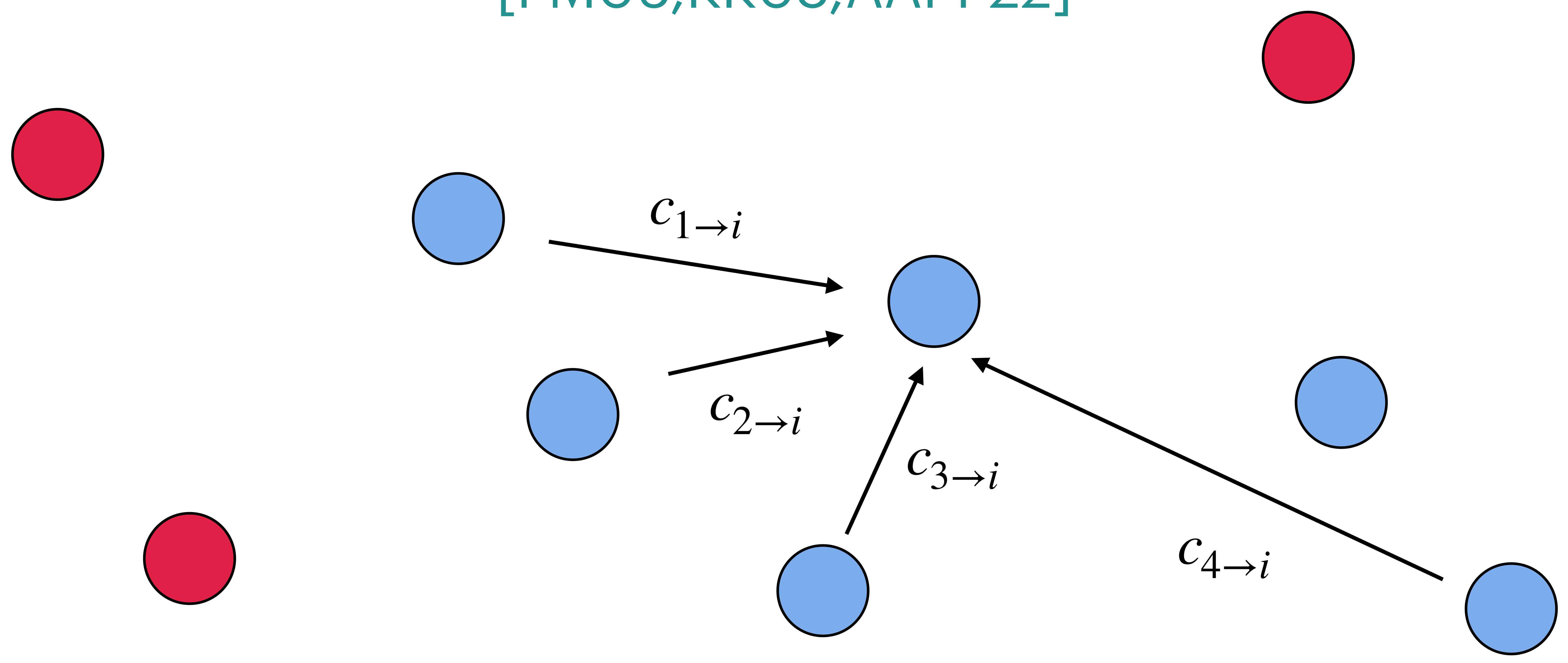
Leader Election from Commitments

[FM06,KK08,AAPP22]



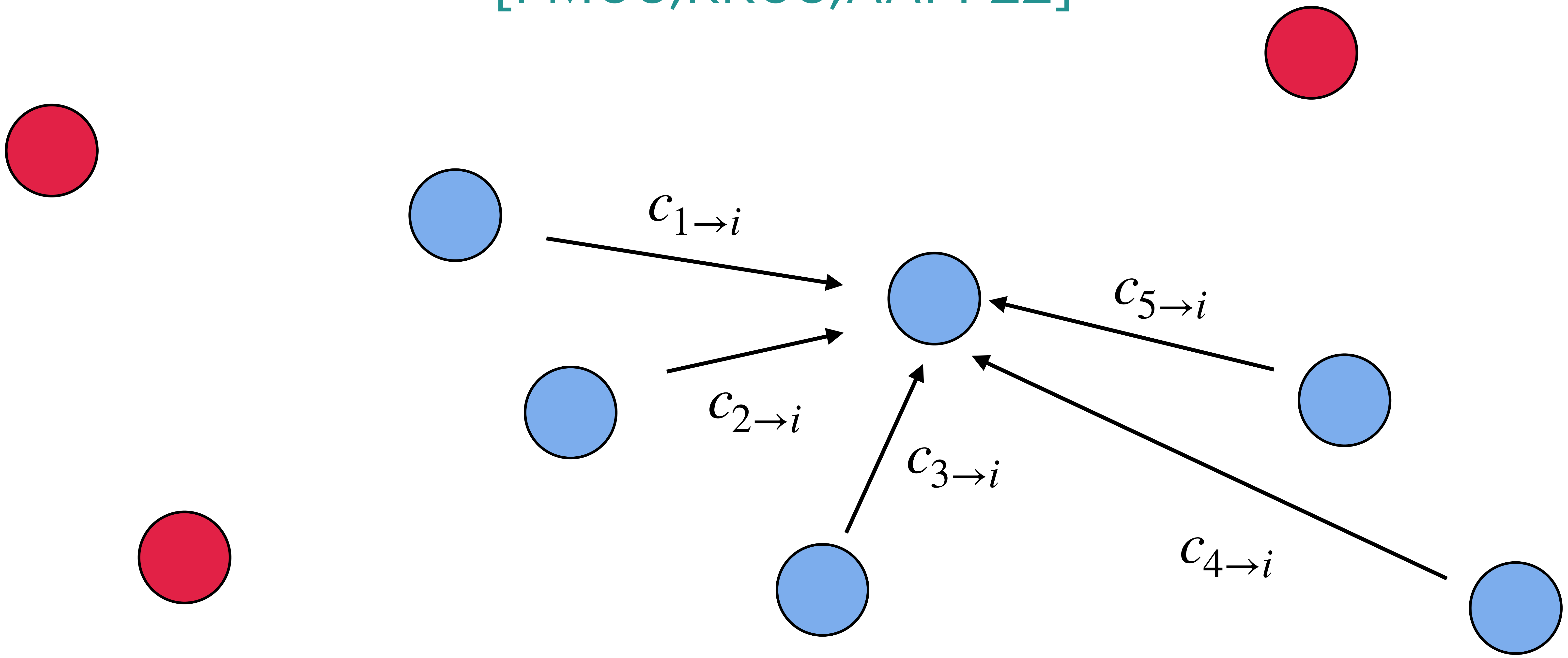
Leader Election from Commitments

[FM06,KK08,AAPP22]



Leader Election from Commitments

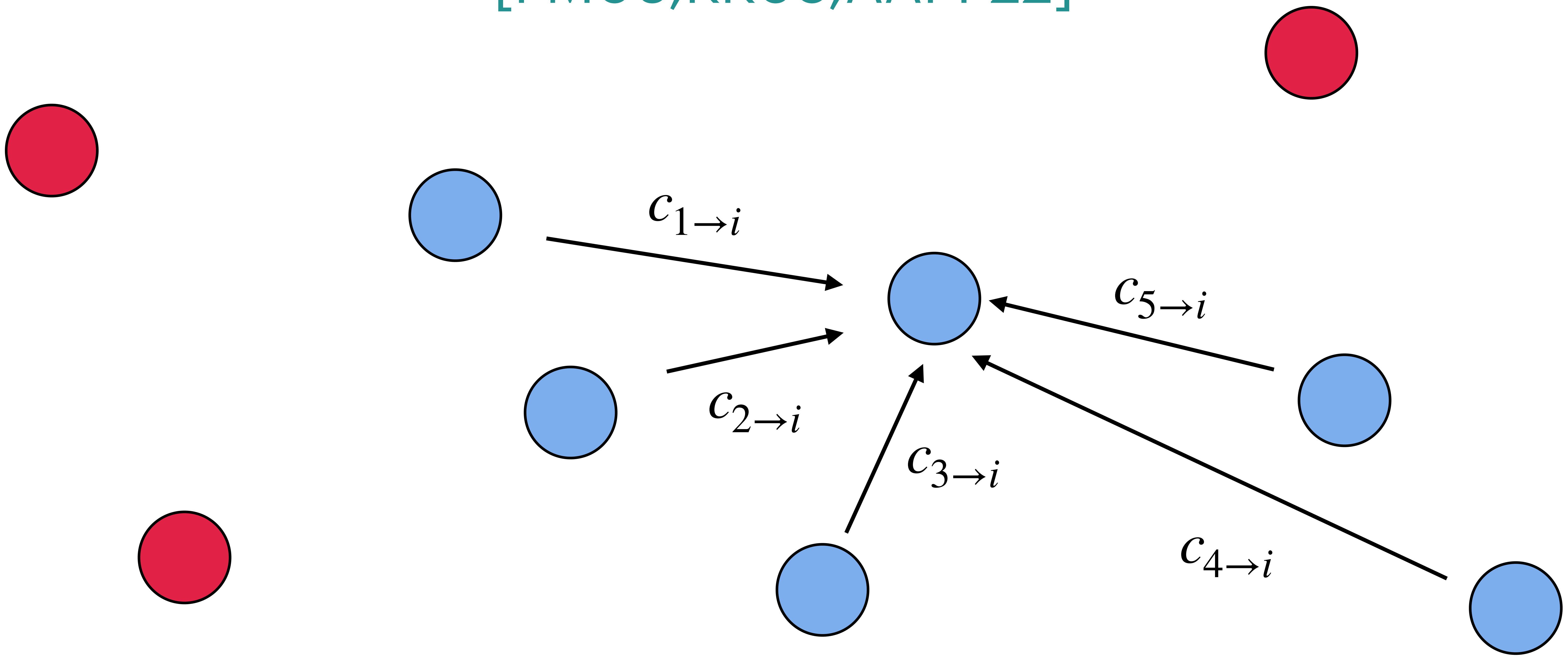
[FM06,KK08,AAPP22]



Contribution via
commit + reveal

…lection from Commitments

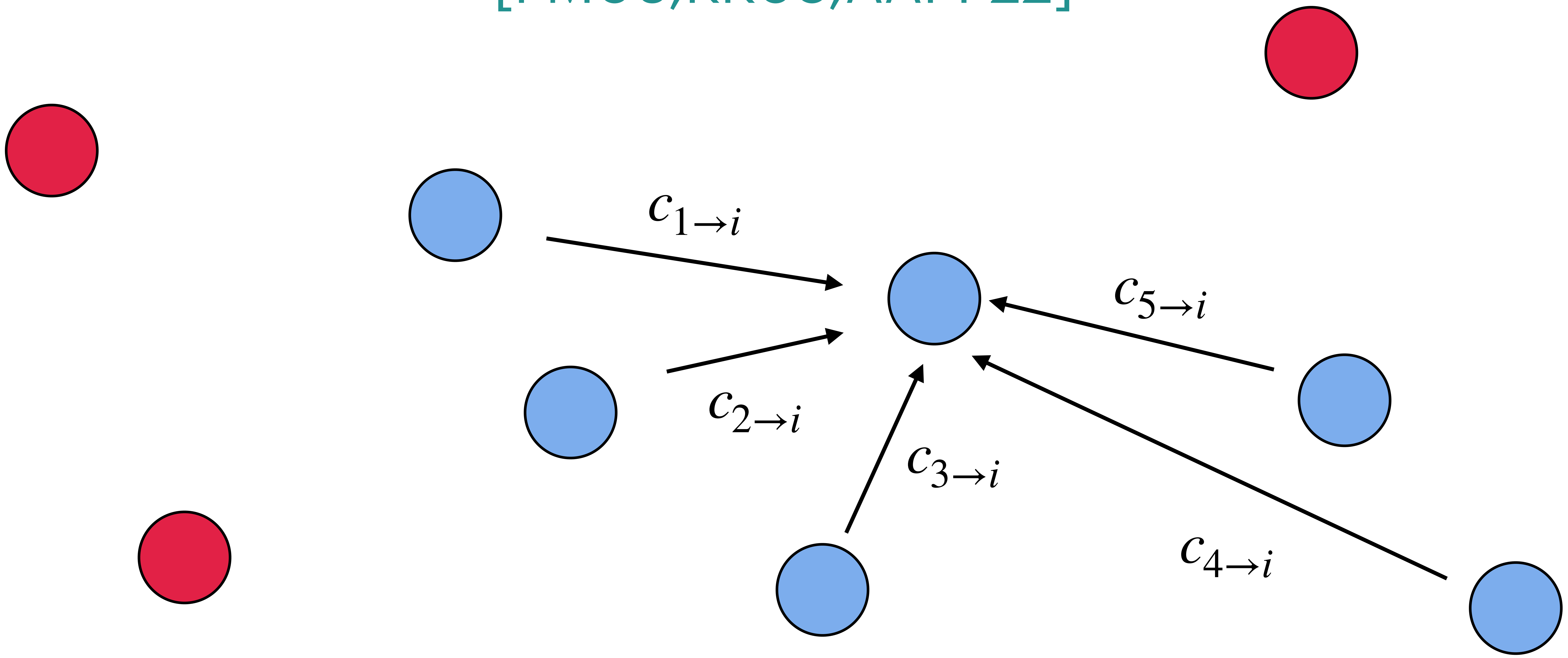
[FM06,KK08,AAPP22]



Contribution via
commit + reveal

lection from Commitments

[FM06,KK08,AAPP22]

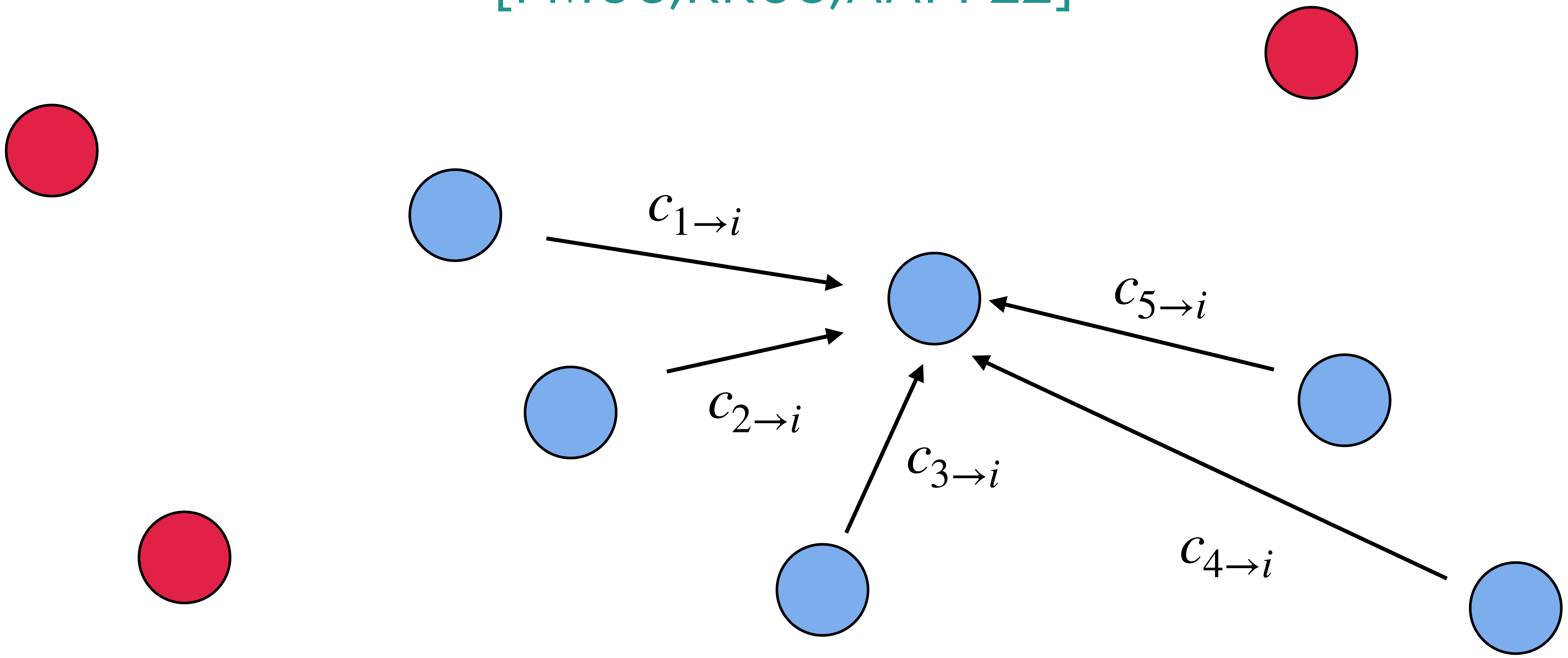


$$c_i = \sum_{j=1}^{n} c_{j\to i}$$

lection from Commitments

Contribution via
commit + reveal

[FM06,KK08,AAPP22]



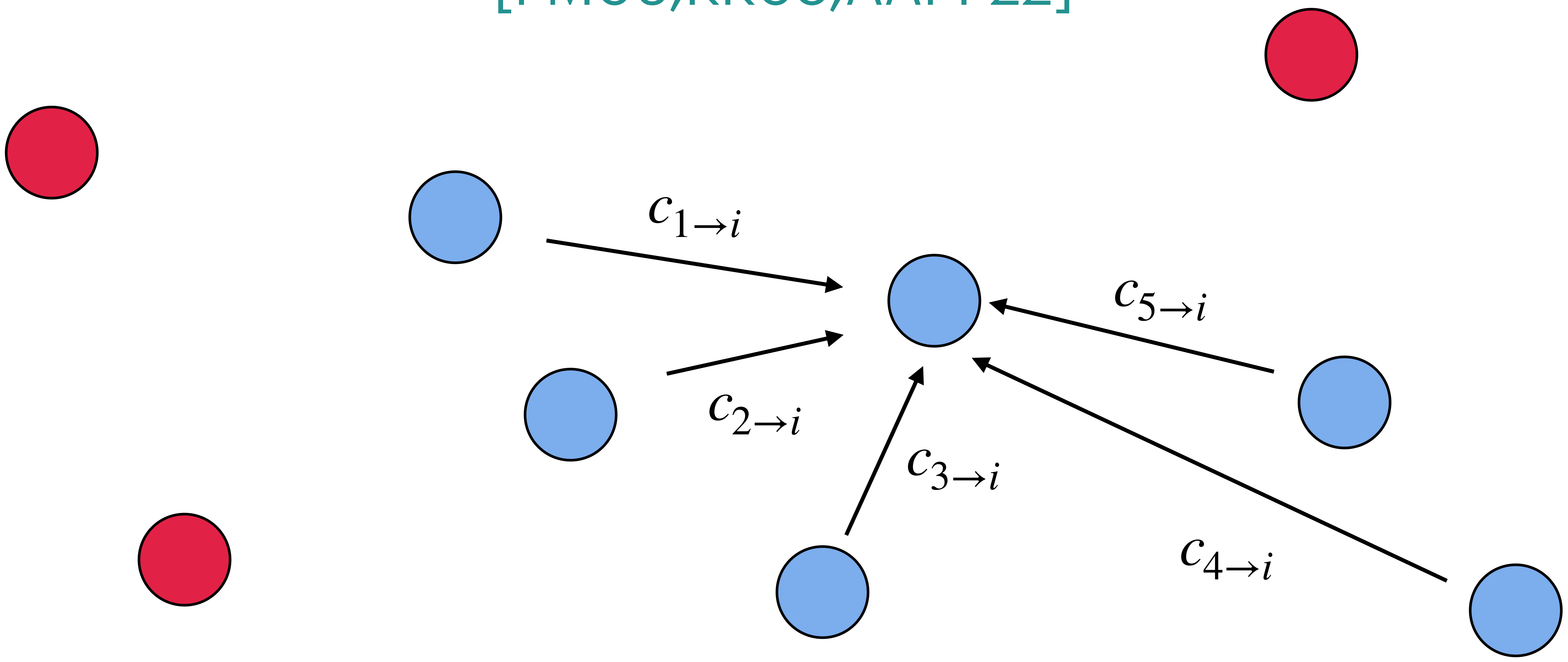
Adversary cannot bias!

$$c_i = \sum_{j=1}^{n} c_{j\to i}$$

Contribution via
commit + reveal

…lection from Commitments

[FM06,KK08,AAPP22]

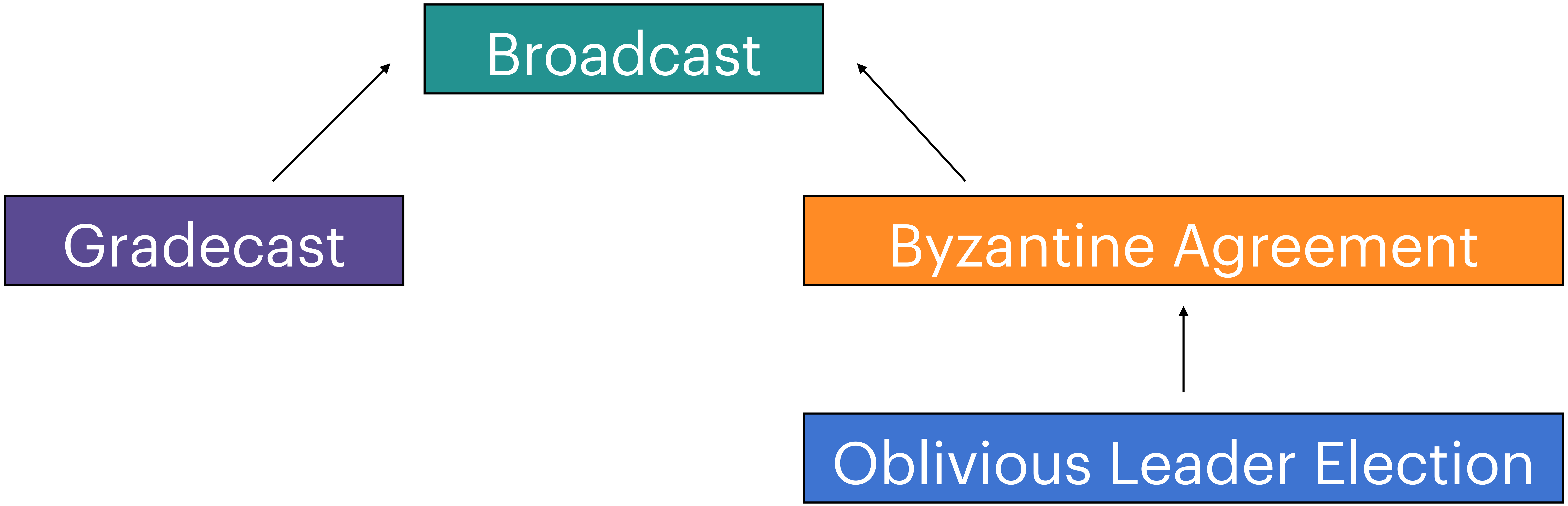


Adversary cannot bias!

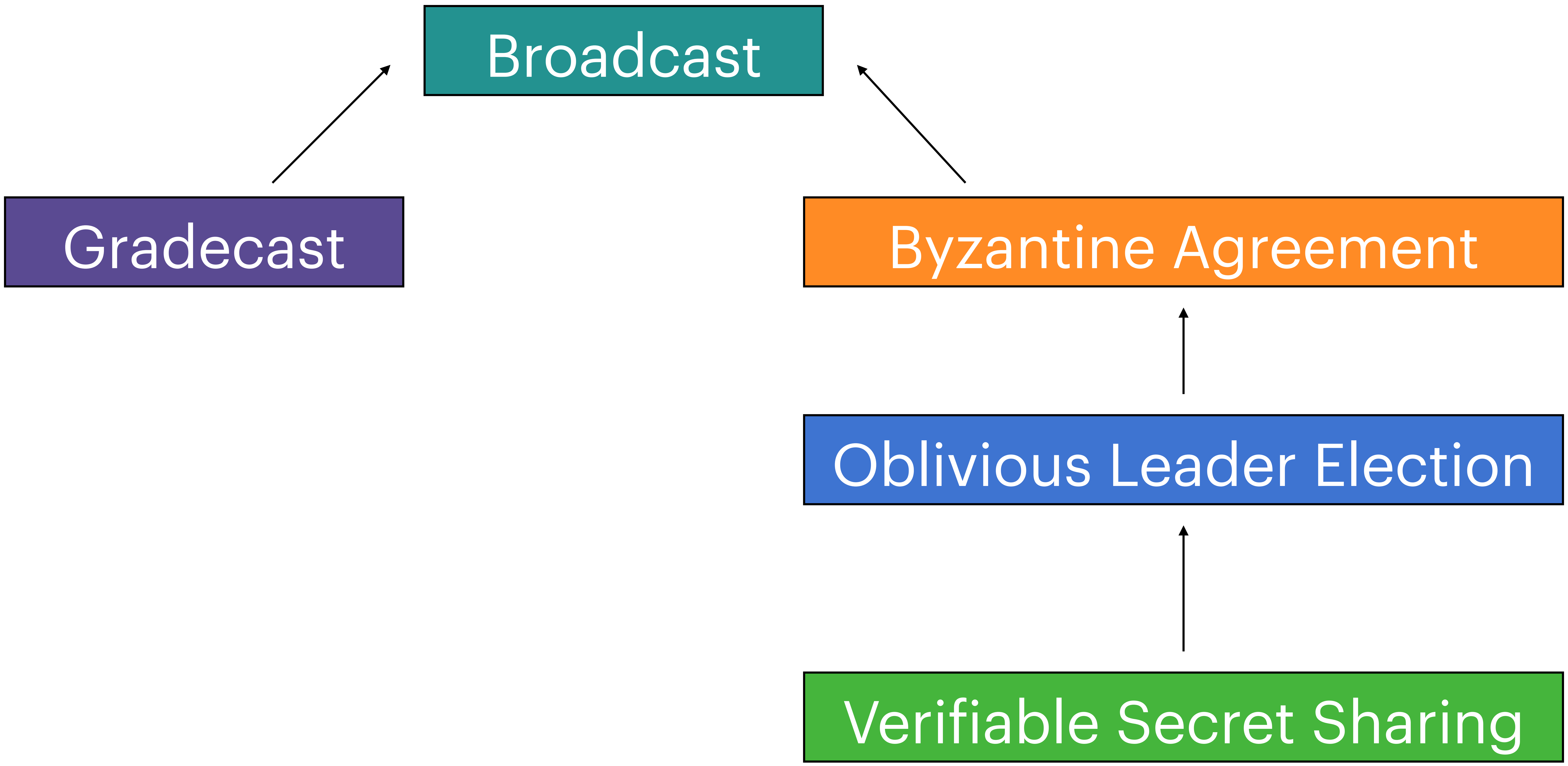
$$c_i = \sum_{j=1}^{n} c_{j\to i}$$

Each party receives at least one uniformly random contribution from an honest party

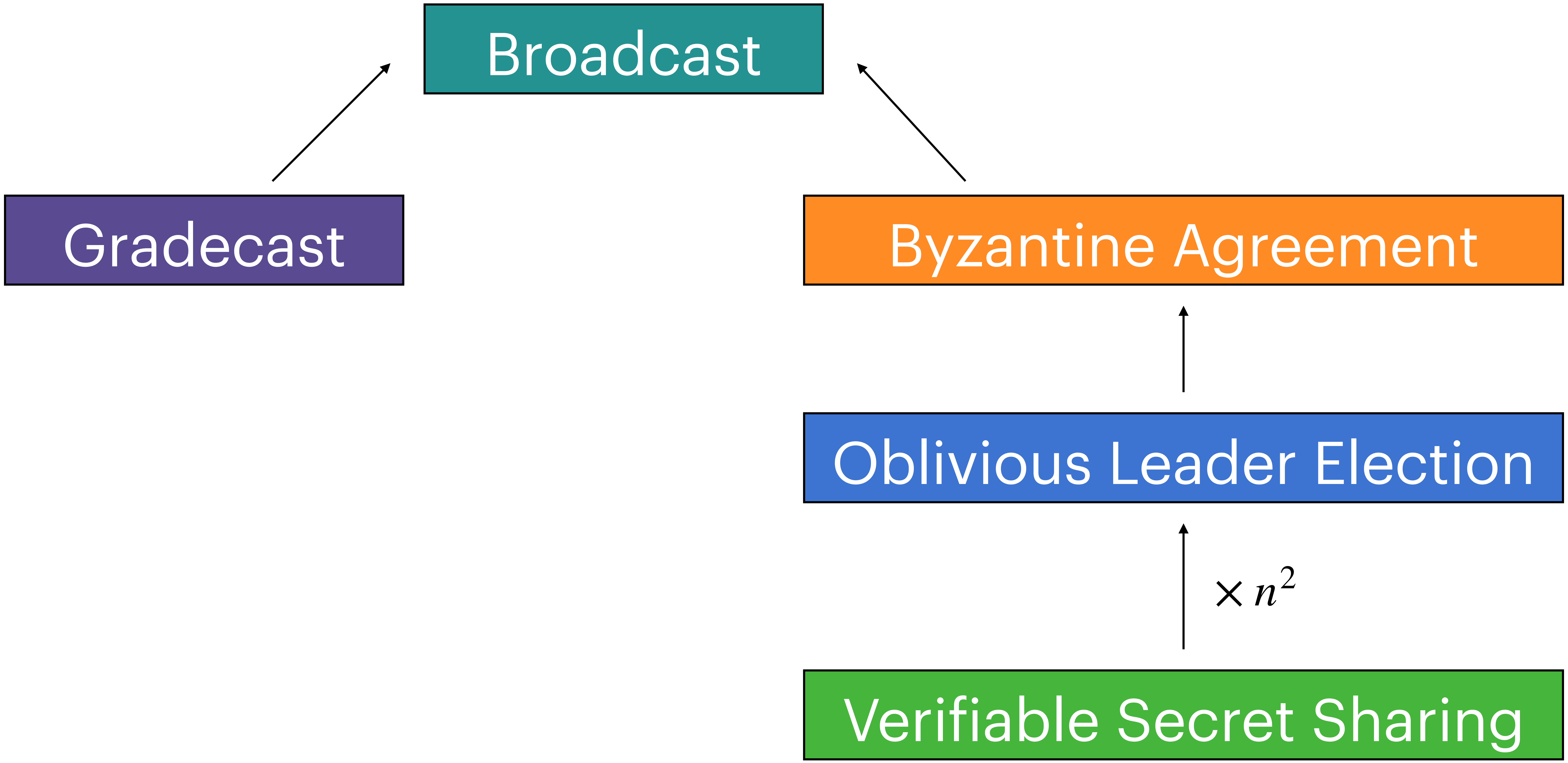
[KK06] Framework



[KK06] Framework



[KK06] Framework



$$\Pr[\text{Everyone agrees on honest leader}] \geq \frac{1}{2}$$

$$\mathsf{Pr}[\text{Everyone agrees on honest leader}] \geq \frac{1}{2}$$

$$\mathsf{Pr}[\text{No agreement } \textbf{OR} \text{ corrupted leader}] \leq \frac{1}{2}$$

$$\Pr[\text{Everyone agrees on honest leader}] \geq \frac{1}{2}$$

$$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader}] \leq \frac{1}{2}$$

← Probability that OLE fails!

$$\Pr[\text{Everyone agrees on honest leader}] \geq \frac{1}{2}$$

$$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader}] \leq \frac{1}{2}$$

Probability that OLE fails!

$$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader } \textbf{OR} \text{ some other bad event}] \leq \frac{1}{2}$$

✅ $\Pr[\text{Everyone agrees on honest leader}] \geq \frac{1}{2}$

$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader}] \leq \frac{1}{2}$ ← Probability that OLE fails!

$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader } \textbf{OR} \text{ some other bad event}] \leq \frac{1}{2}$

$$\Pr[\text{Everyone agrees on honest leader}] \geq \frac{1}{2}$$

$$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader}] \leq \frac{1}{2}$$

Probability that OLE fails!

$$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader } \textbf{OR} \text{ some other bad event}] \leq \frac{1}{2}$$

Statistical security suffices!

$\Pr[\text{Everyone agrees on honest leader}] \geq \frac{1}{2}$

$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader}] \leq \frac{1}{2}$ ← Probability that OLE fails!

$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader } \textbf{OR} \text{ some other bad event}] \leq \frac{1}{2}$

↑ Statistical error

Statistical security suffices!

$$\Pr[\text{Everyone agrees on honest leader}] \geq \frac{1}{2}$$

$$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader}] \leq \frac{1}{2}$$

Probability that OLE fails!

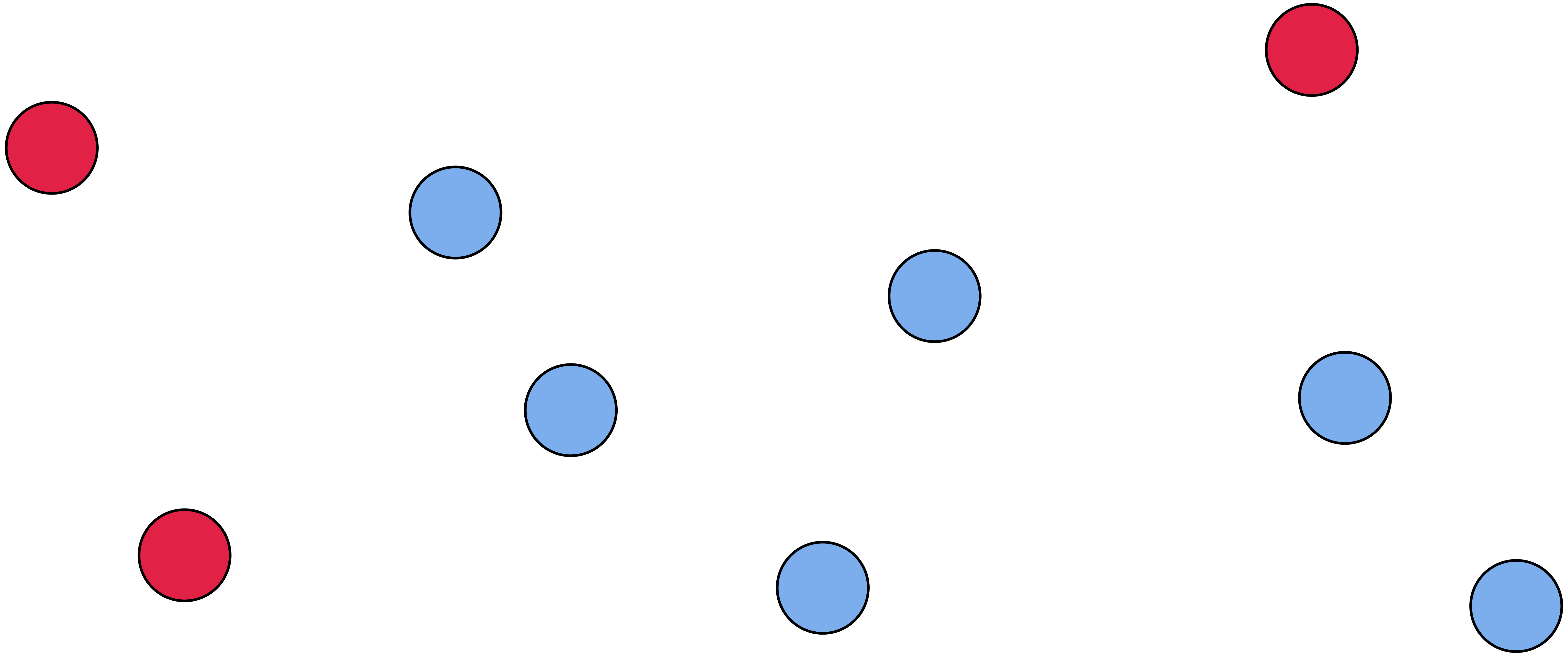
$$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader } \textbf{OR} \text{ some other bad event}] \leq \frac{1}{2}$$

Statistical error

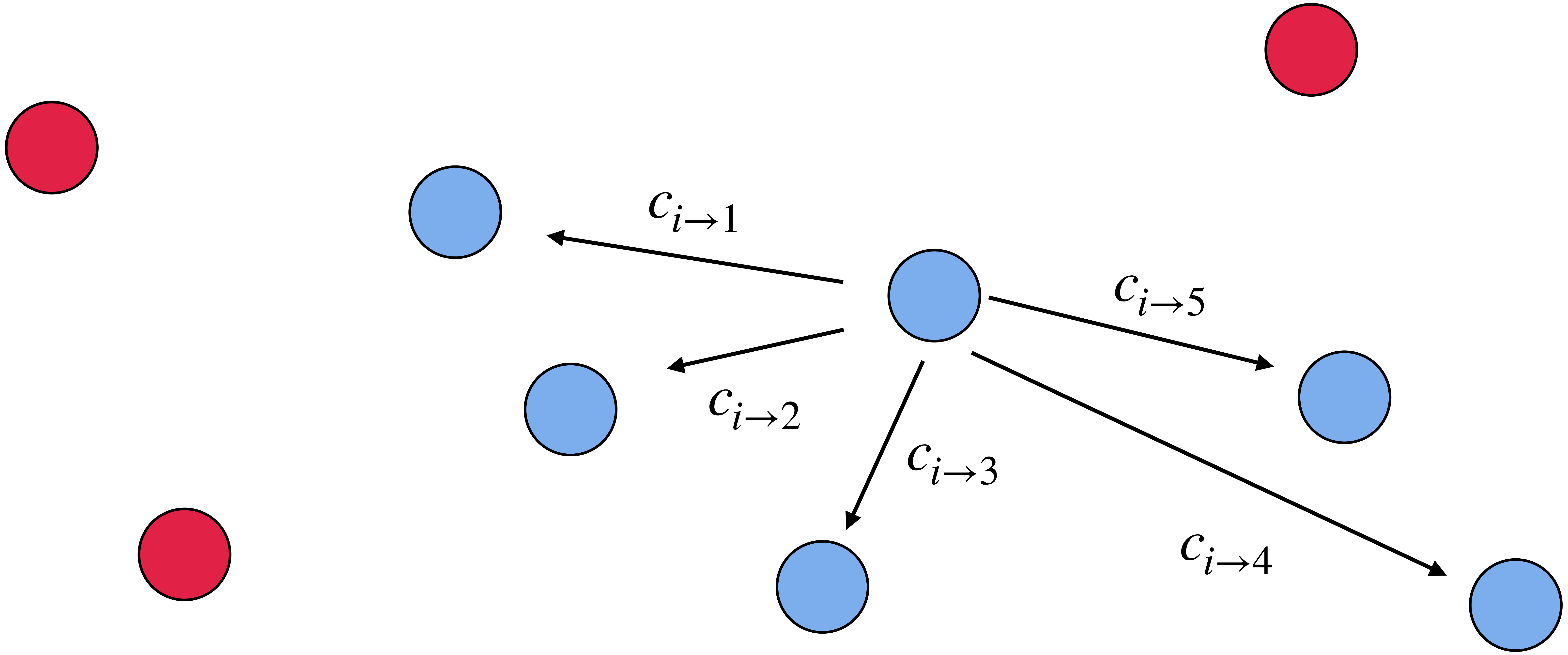
Statistical security suffices!

Leads to fewer secrets!

Reducing the # of Secrets

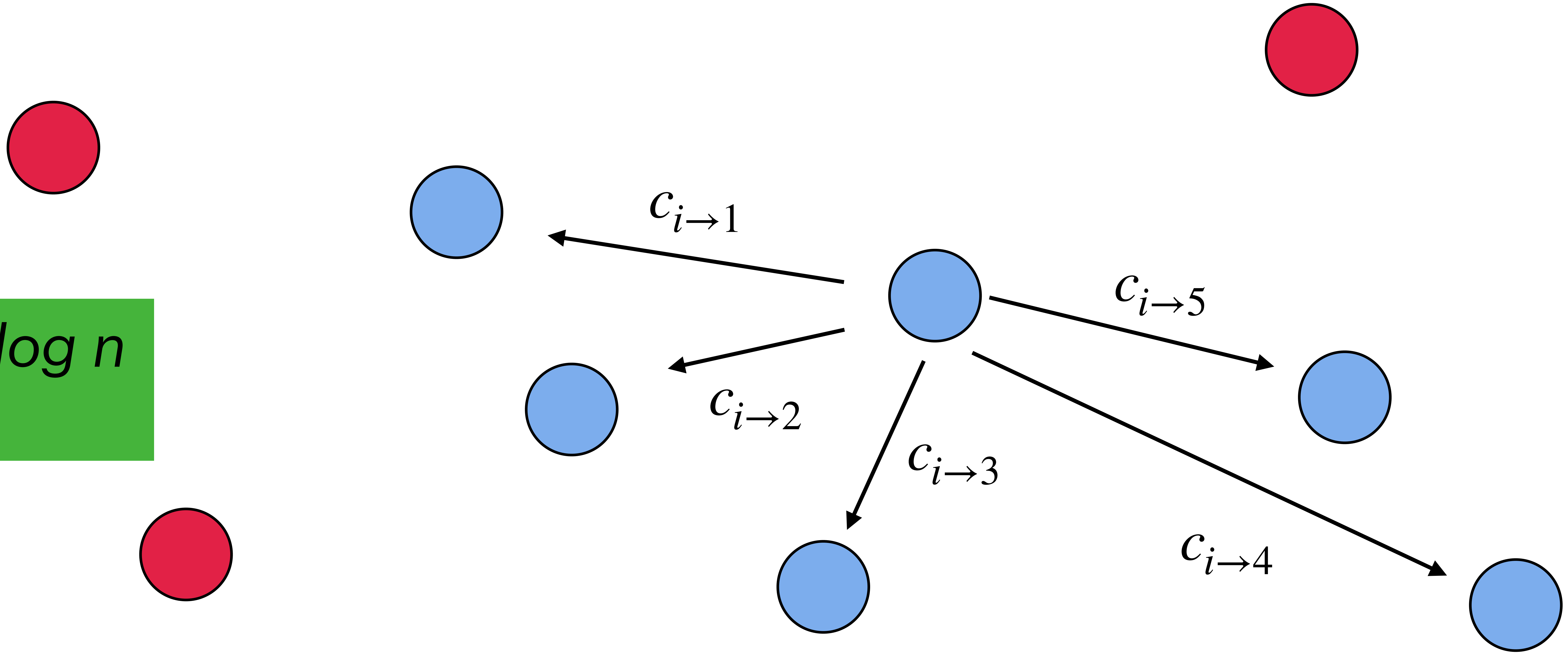


Reducing the # of Secrets



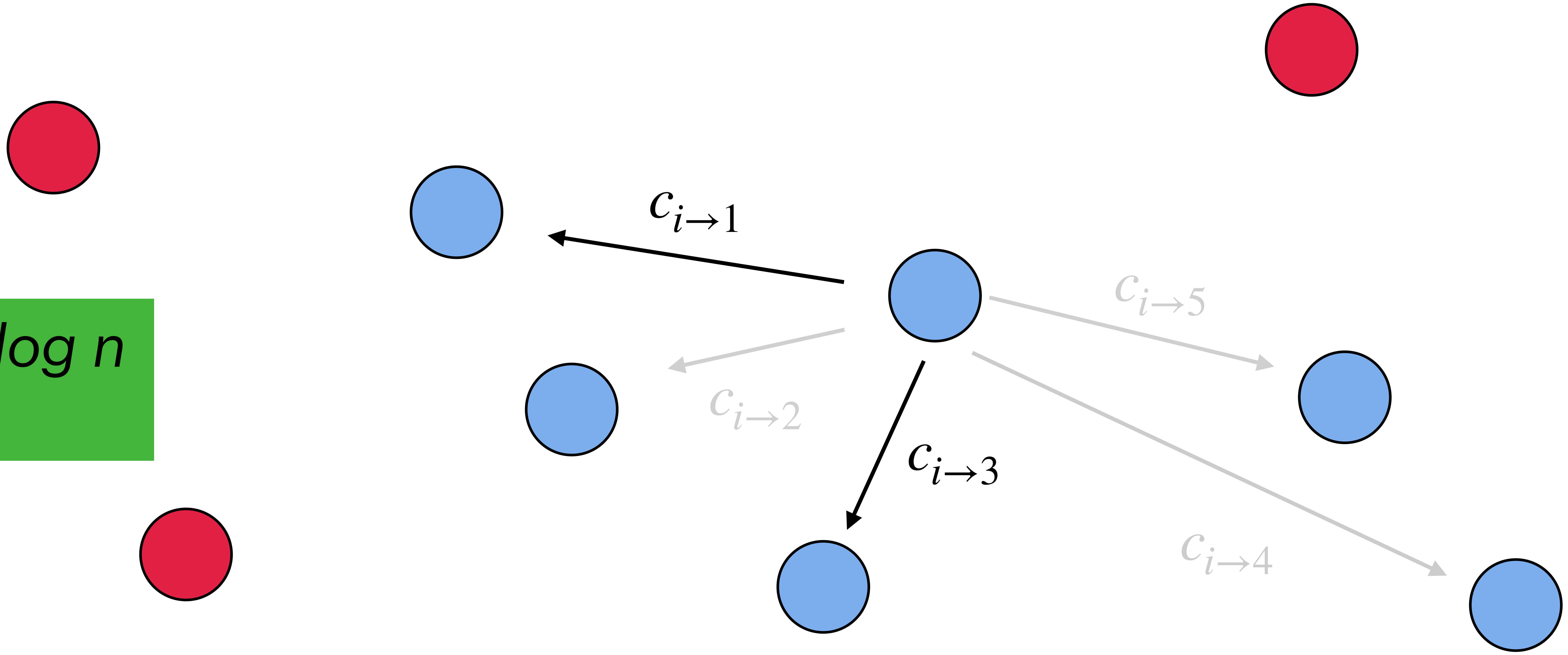
Reducing the # of Secrets

Contribute to *log n* parties!

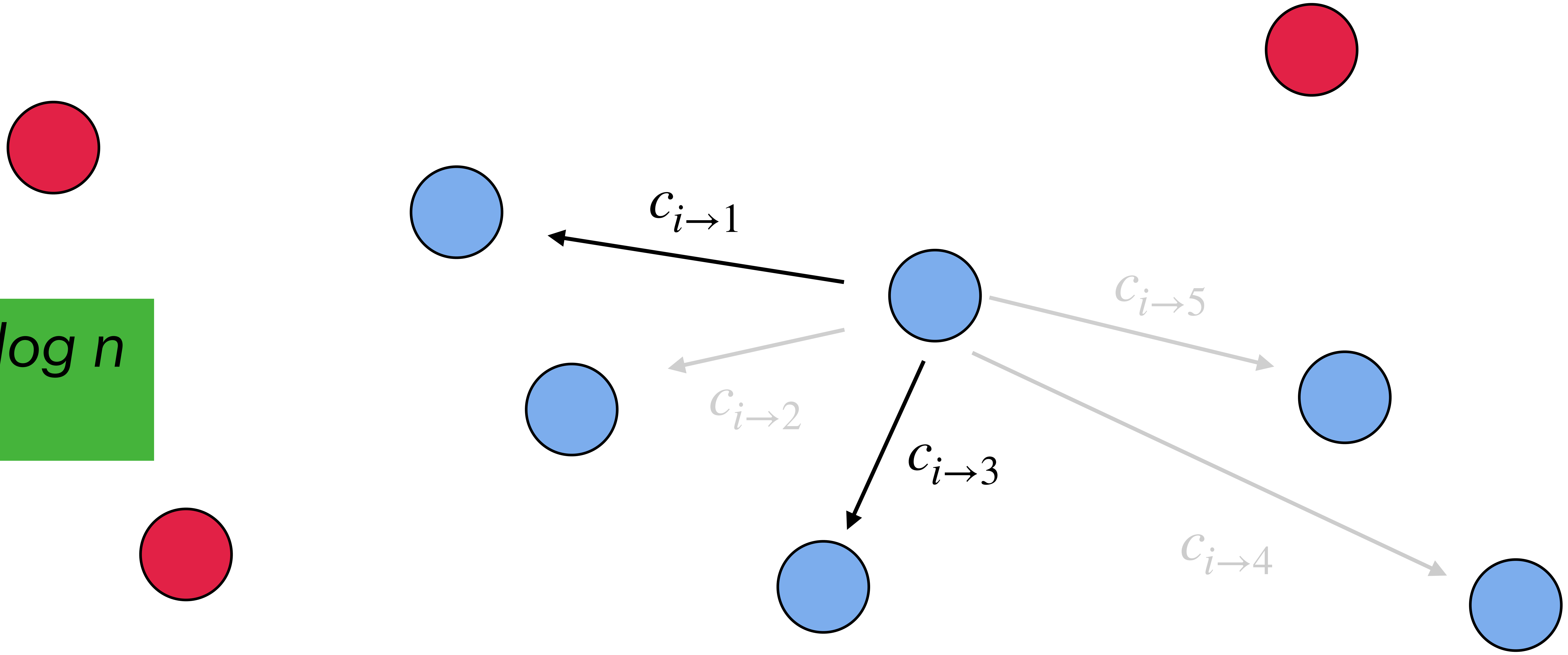


Reducing the # of Secrets

Contribute to *log n* parties!



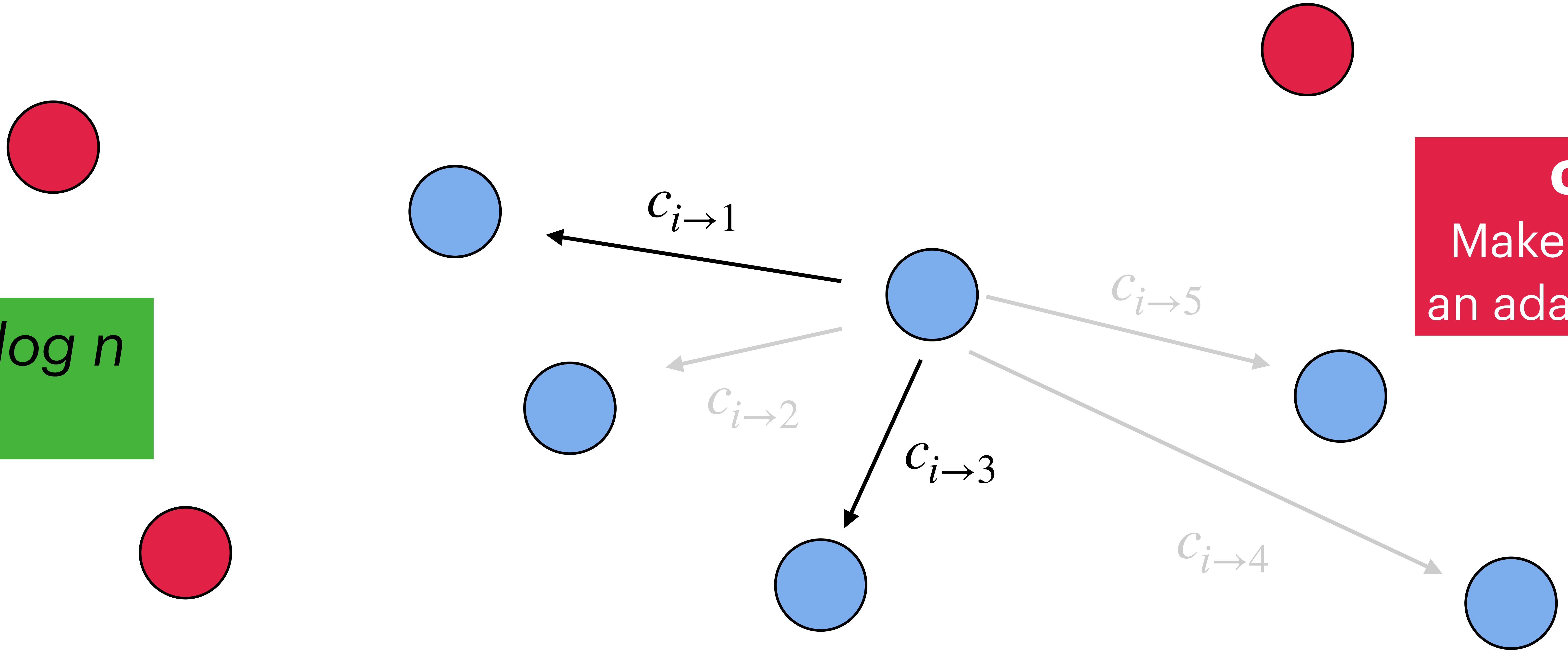
Reducing the # of Secrets



Contribute to *log n* parties!

We need: With high probability each party receives at least one honest contribution

Reducing the # of Secrets

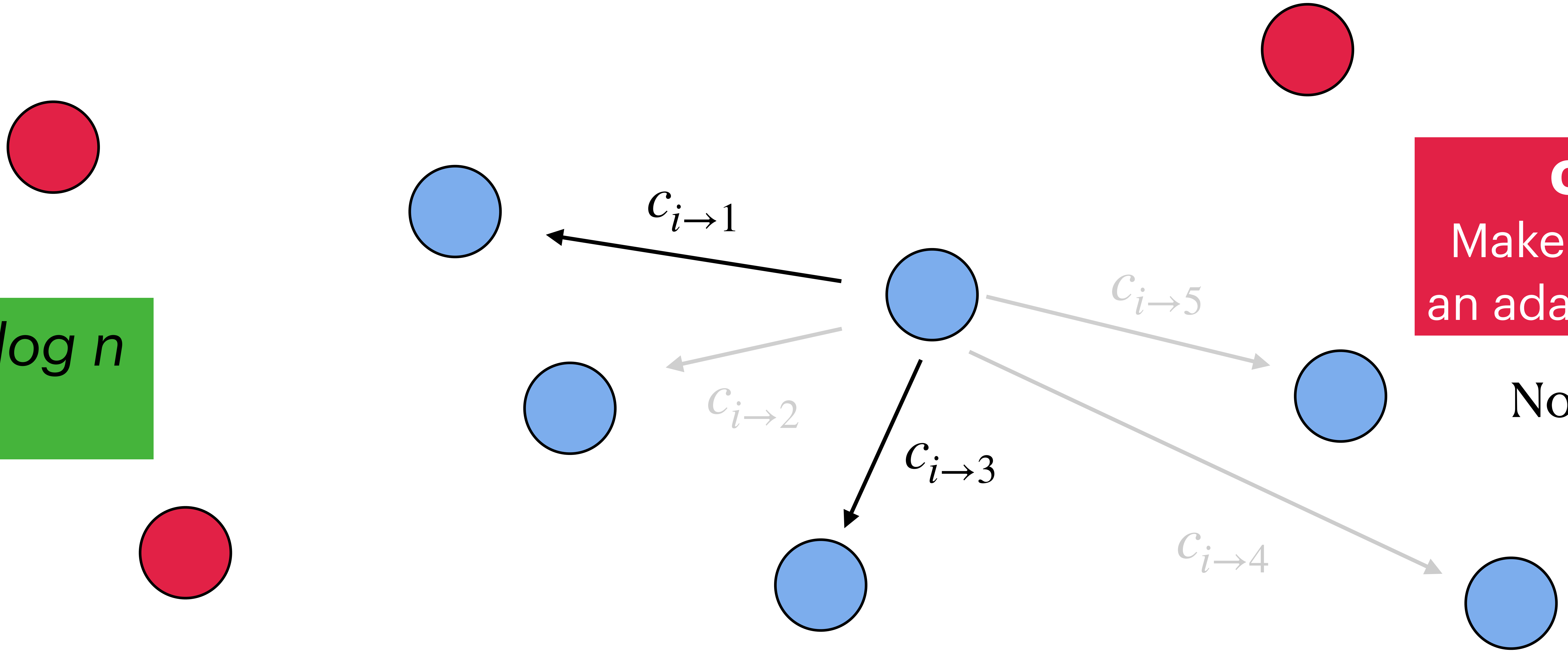


Contribute to *log n* parties!

Challenge
Make it work against an adaptive adversary

We need: With high probability each party receives at least one honest contribution

Reducing the # of Secrets



Contribute to *log n* parties!

Challenge
Make it work against an adaptive adversary

Not in this talk

We need: With high probability each party receives at least one honest contribution

Probability Analysis

Probability Analysis

Each party contributes to *log n* parties chosen uniformly at random

Probability Analysis

Each party contributes to *log n* parties chosen uniformly at random

$$\Pr[\text{No honest } j \text{ contributes to } i] \leq \left(\left(1 - \frac{1}{n}\right)^{\log n}\right)^{2n/3} \leq e^{-\log n}$$

Probability Analysis

Each party contributes to *log n* parties chosen uniformly at random

$$\Pr[\text{No honest } j \text{ contributes to } i] \leq \left(\left(1 - \frac{1}{n}\right)^{\log n}\right)^{2n/3} \leq e^{-\log n}$$

Probability that *j* does not pick *i* once

Probability Analysis

Each party contributes to *log n* parties chosen uniformly at random

For *log n* independent samples

$$\Pr[\text{No honest } j \text{ contributes to } i] \leq \left(\left(1 - \frac{1}{n}\right)^{\log n}\right)^{2n/3} \leq e^{-\log n}$$

Probability that *j* does not pick *i* once

Probability Analysis

Each party contributes to *log n* parties chosen uniformly at random

For *log n* independent samples

# of honest parties

$$\Pr[\text{No honest } j \text{ contributes to } i] \leq \left(\left(1 - \frac{1}{n}\right)^{\log n} \right)^{2n/3} \leq e^{-\log n}$$

Probability that *j* does not pick *i* once

Probability Analysis

Each party contributes to *log n* parties chosen uniformly at random

For *log n* independent samples

# of honest parties

$$\Pr[\text{No honest } j \text{ contributes to } i] \leq \left(\left(1 - \frac{1}{n}\right)^{\log n}\right)^{2n/3} \leq e^{-\log n}$$

Probability that *j* does not pick *i* once

$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader } \textbf{OR} \text{ for some } i \text{ no honest } j \text{ contributes}] \leq \frac{1}{2}$

Probability Analysis

Each party contributes to *log n* parties chosen uniformly at random

For *log n* independent samples

\# of honest parties

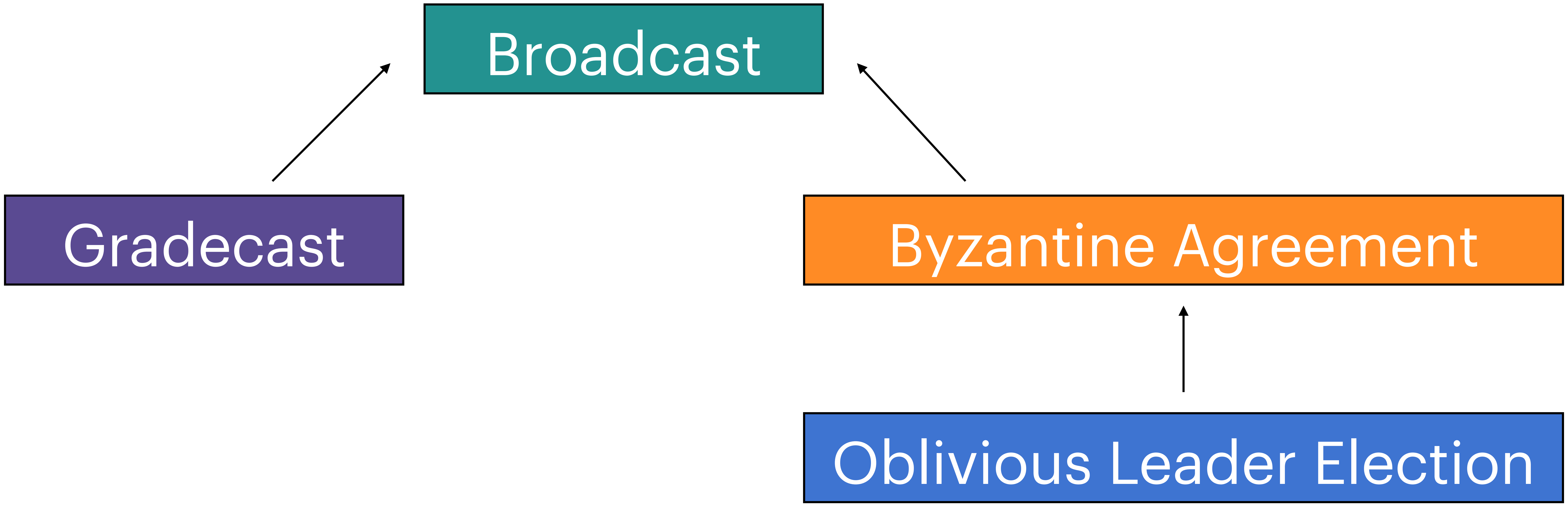
$$\Pr[\text{No honest } j \text{ contributes to } i] \leq \left(\left(1 - \frac{1}{n}\right)^{\log n}\right)^{2n/3} \leq e^{-\log n}$$

Probability that *j* does not pick *i* once

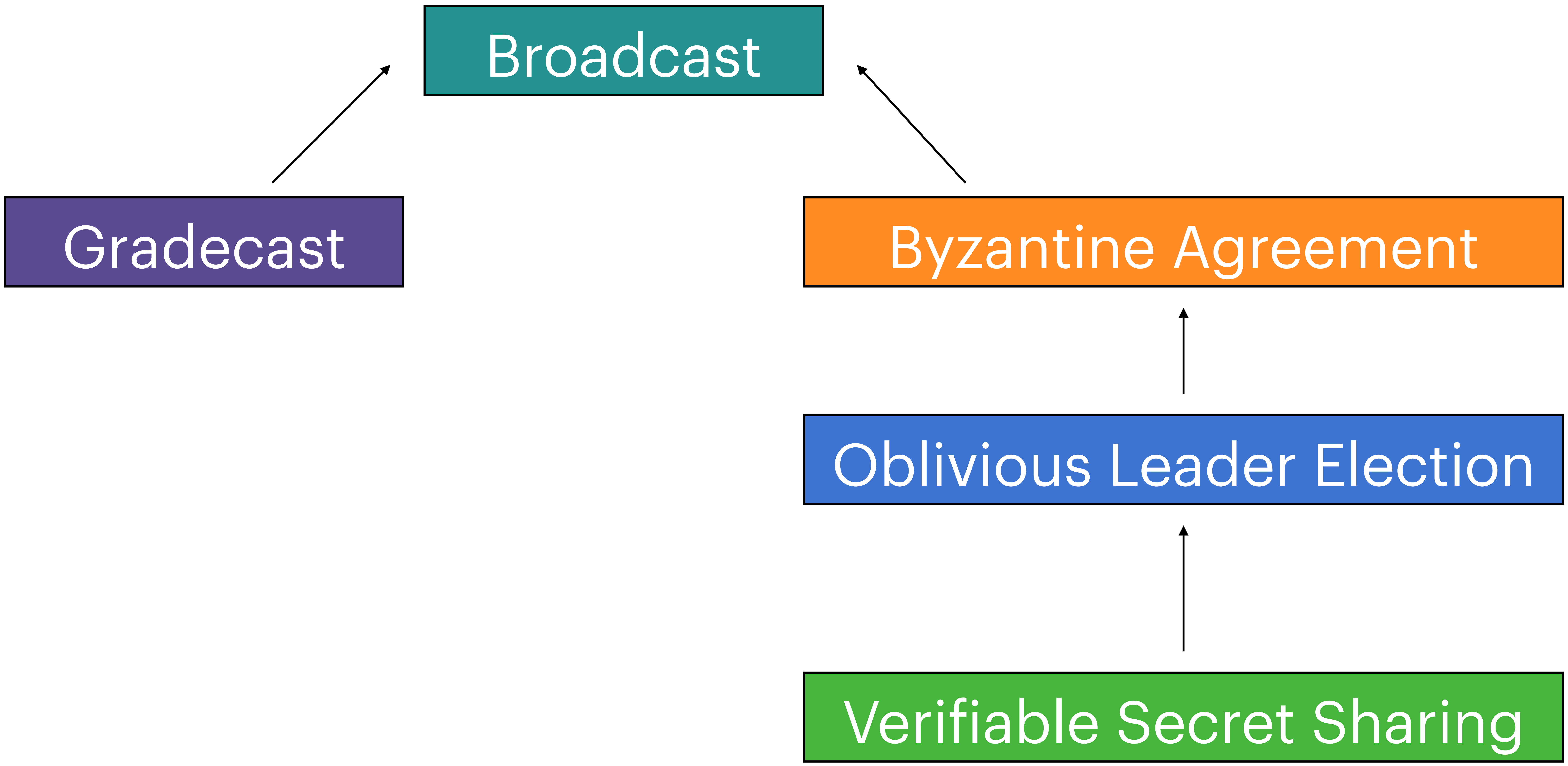
$\leq n \cdot e^{-\log n}$

$$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader } \textbf{OR} \text{ for some } i \text{ no honest } j \text{ contributes}] \leq \frac{1}{2}$$

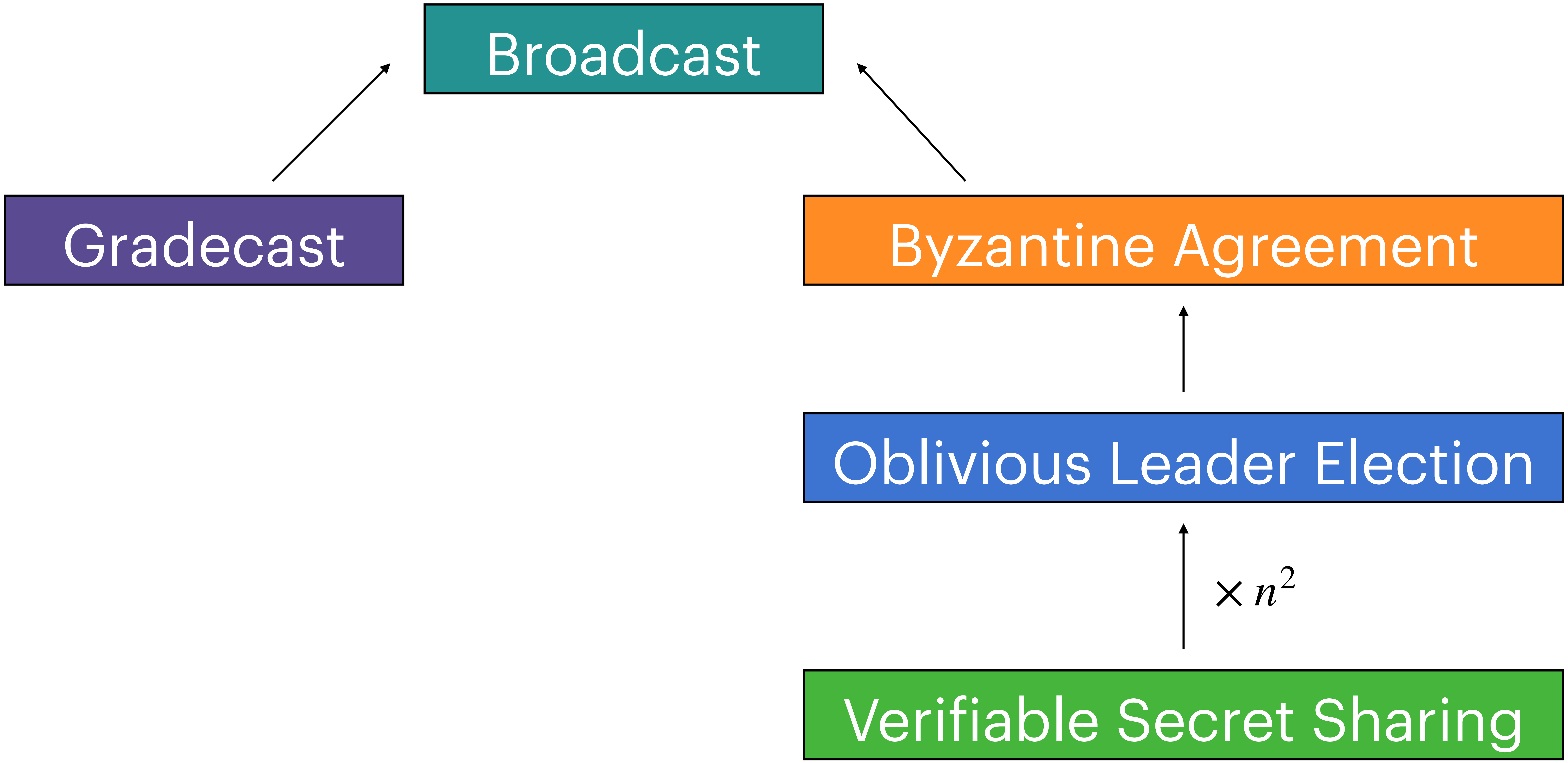
[KK06] Framework



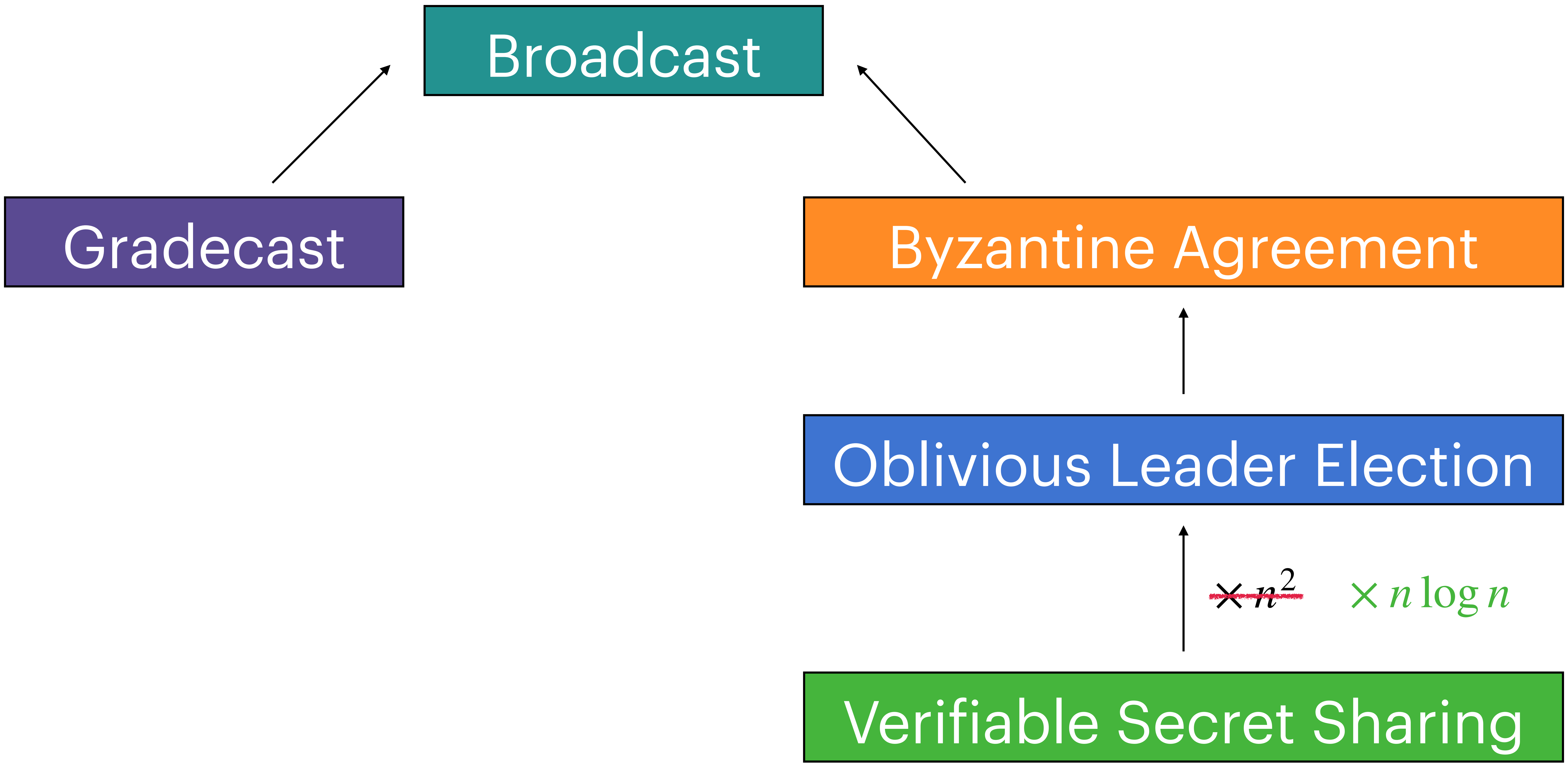
[KK06] Framework



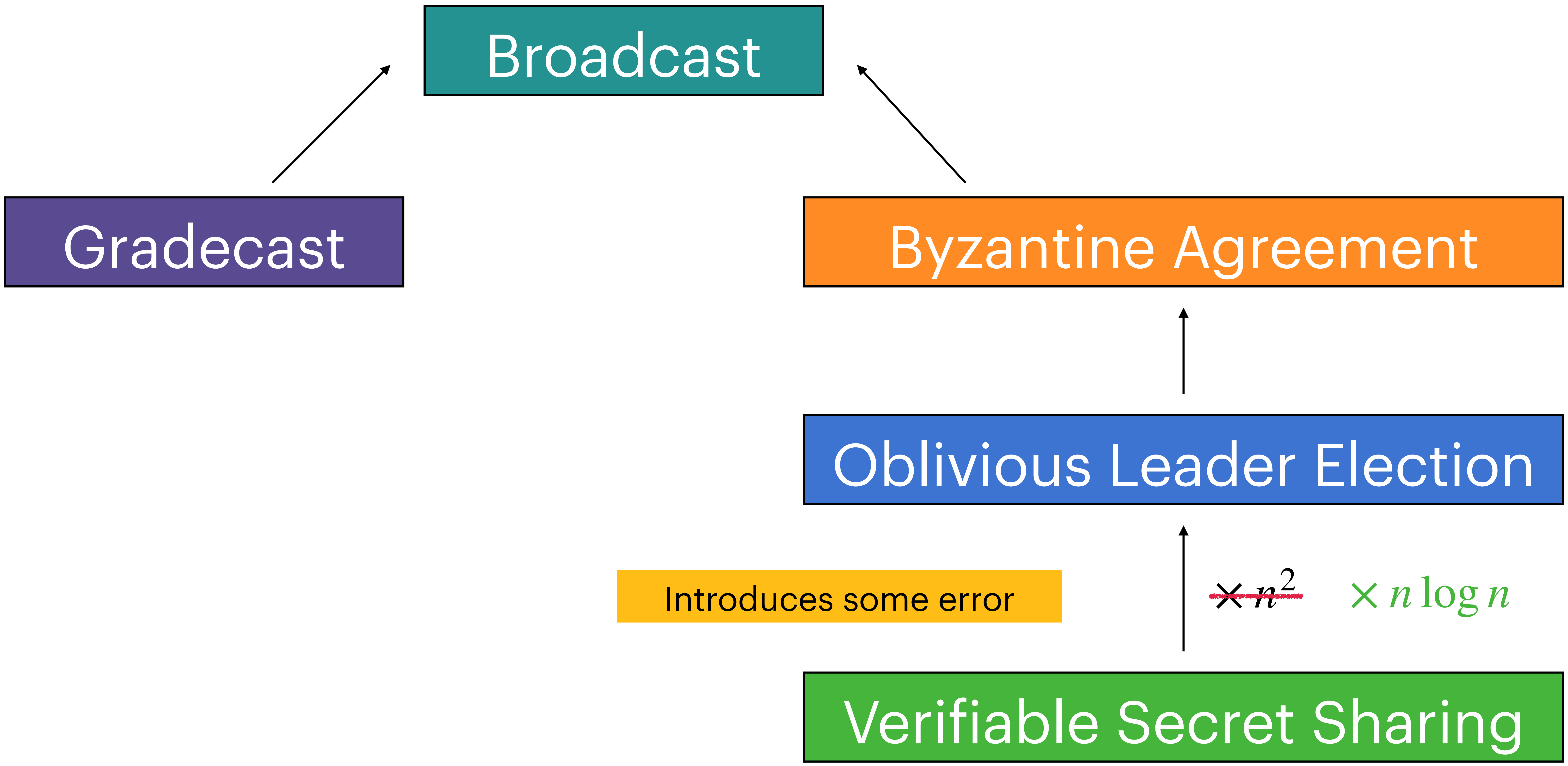
[KK06] Framework



[KK06] Framework



[KK06] Framework



Contributions

- **Conceptual contributions:**
  - Statistical OLE suffices
- **Technical contributions:**
  - Statistical OLE with lesser secrets

Verifiable Secret Sharing

Verifiable Secret Sharing

Information Theoretic Commitments!

Verifiable Secret Sharing

Information Theoretic Commitments!

Dealer

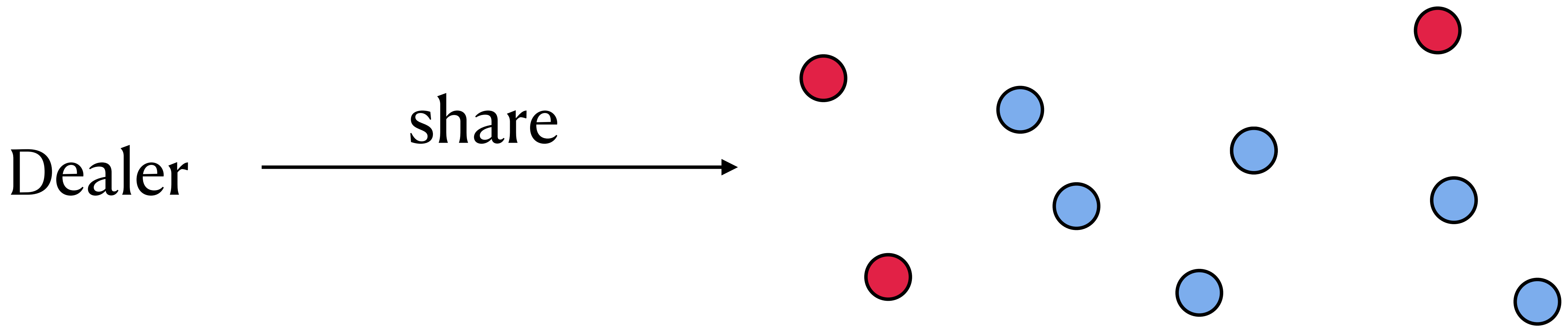
Verifiable Secret Sharing

Information Theoretic Commitments!

Dealer → share

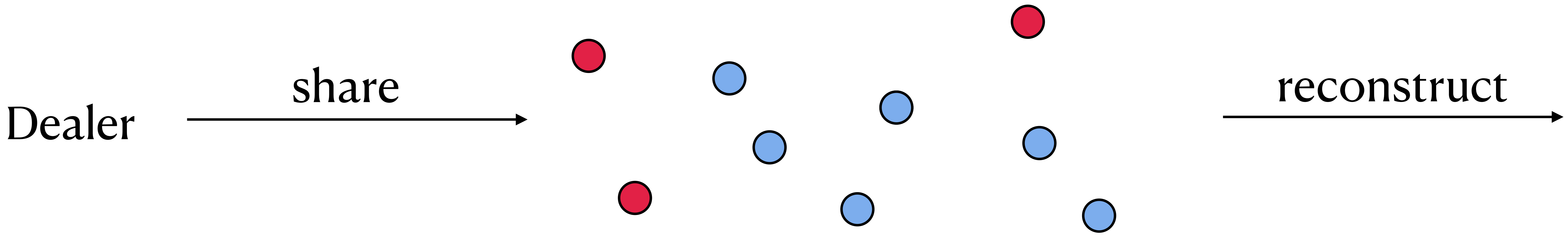
Verifiable Secret Sharing

Information Theoretic Commitments!



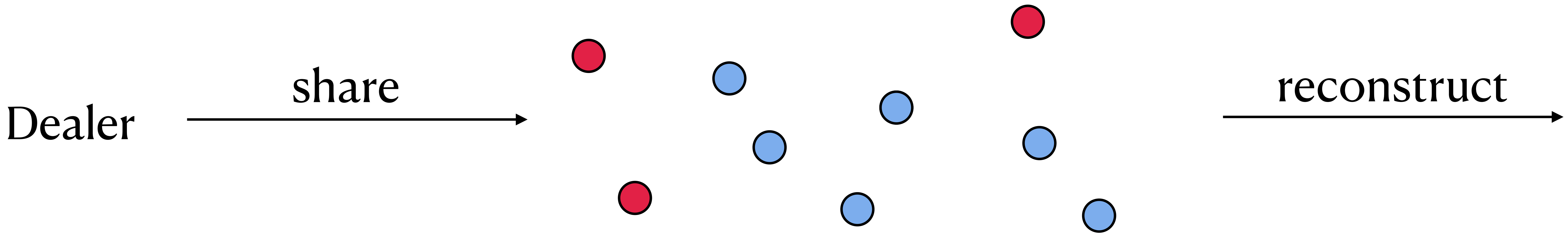
Verifiable Secret Sharing

Information Theoretic Commitments!



Verifiable Secret Sharing

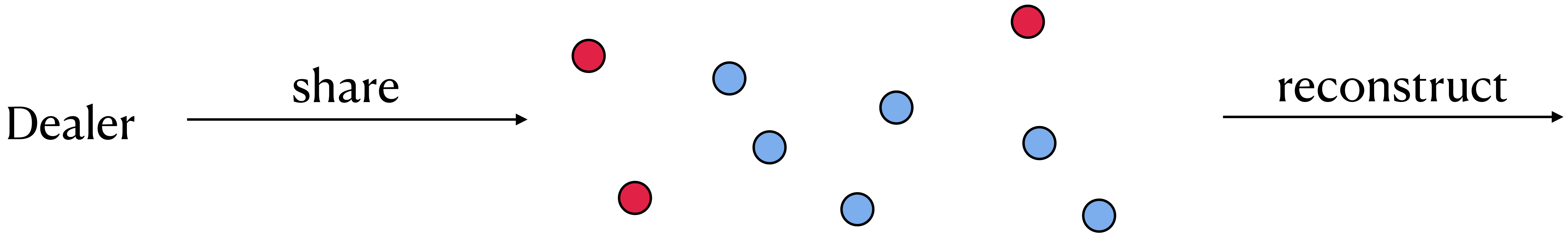
Information Theoretic Commitments!



- Designated dealer can "*share*" a secret *s* among *n* parties
- **Honest dealer:** *s* is private and reconstruction succeeds
- **Corrupt dealer:** Some *s'* is defined and reconstruction succeeds

Verifiable Secret Sharing

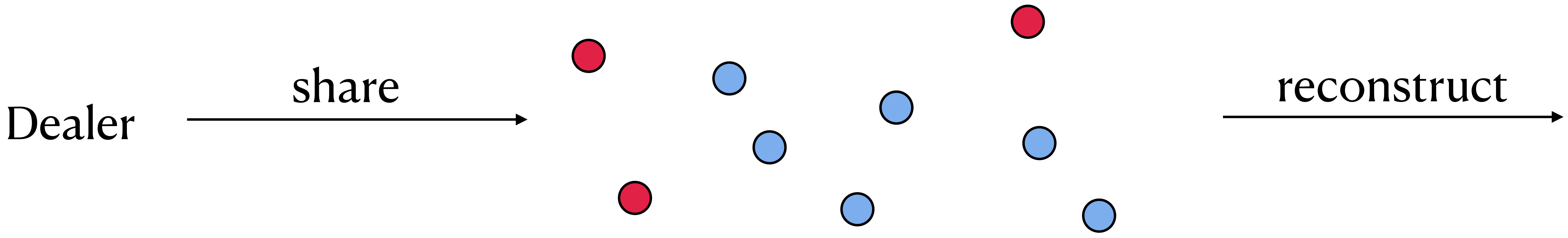
Information Theoretic Commitments!



- Designated dealer can "*share*" a secret *s* among *n* parties
- **Honest dealer:** *s* is private and reconstruction succeeds **Hiding**
- **Corrupt dealer:** Some *s'* is defined and reconstruction succeeds

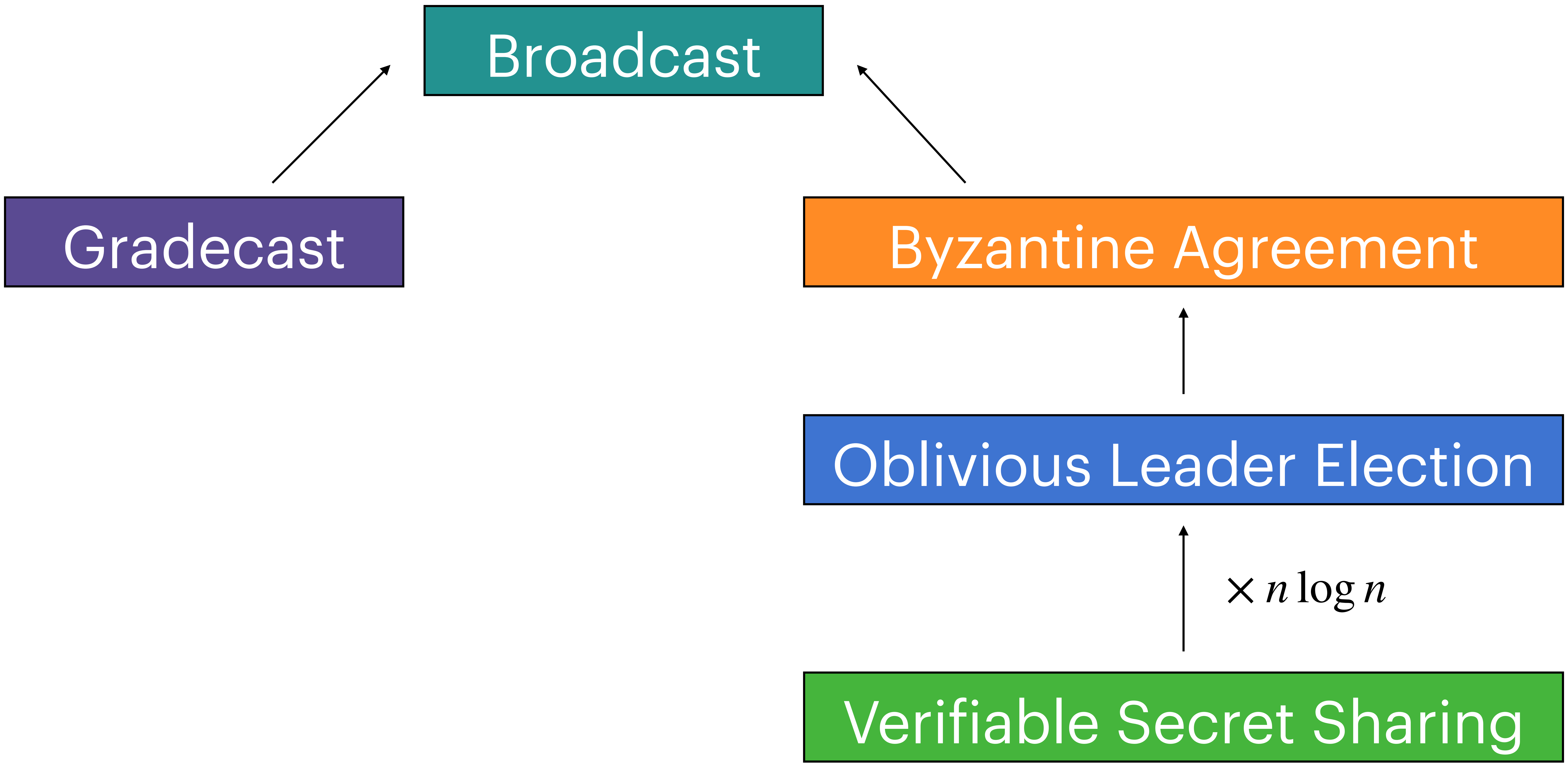
Verifiable Secret Sharing

Information Theoretic Commitments!

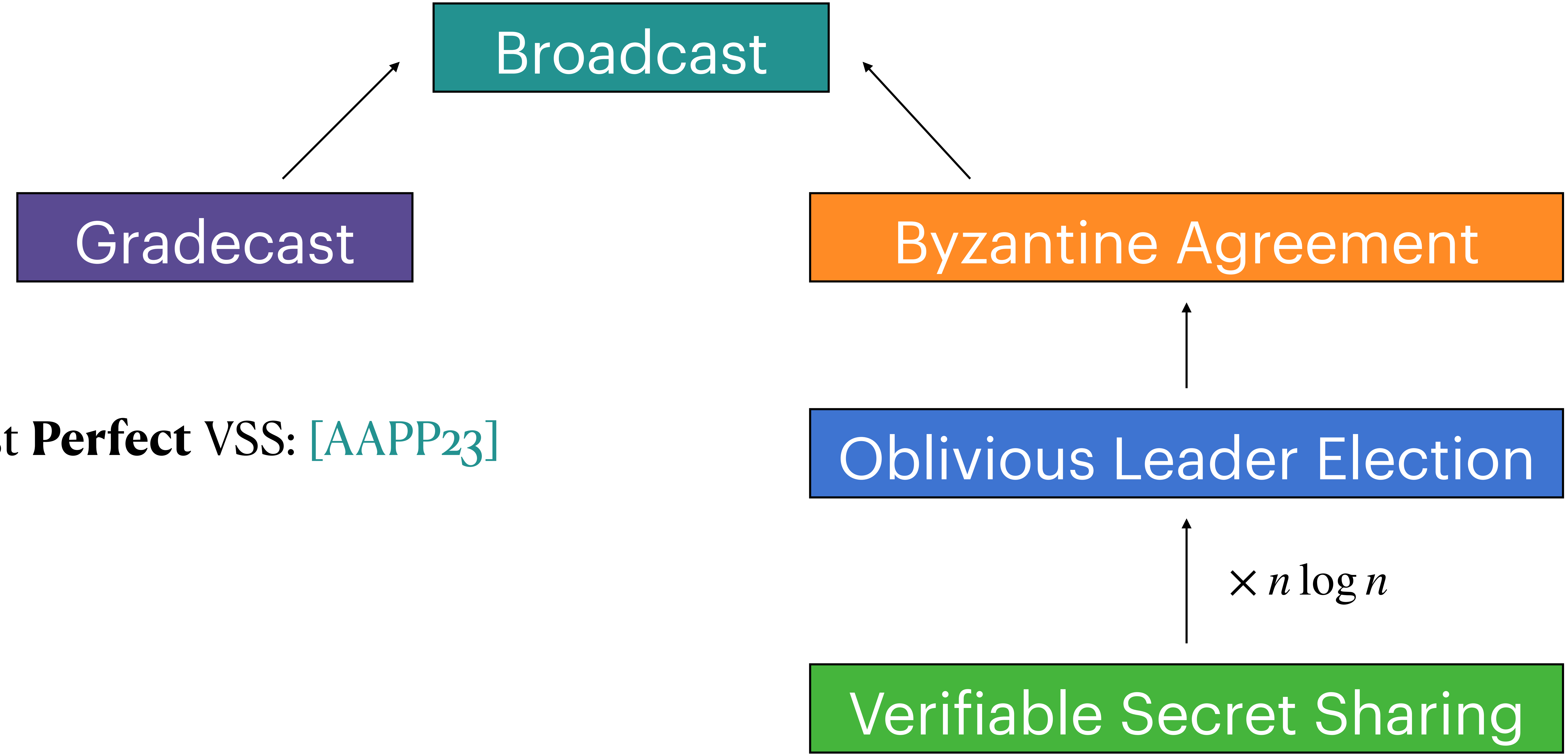


- Designated dealer can "*share*" a secret *s* among *n* parties
- **Honest dealer:** *s* is private and reconstruction succeeds **Hiding**
- **Corrupt dealer:** Some *s'* is defined and reconstruction succeeds **Binding**

[KK06] Framework

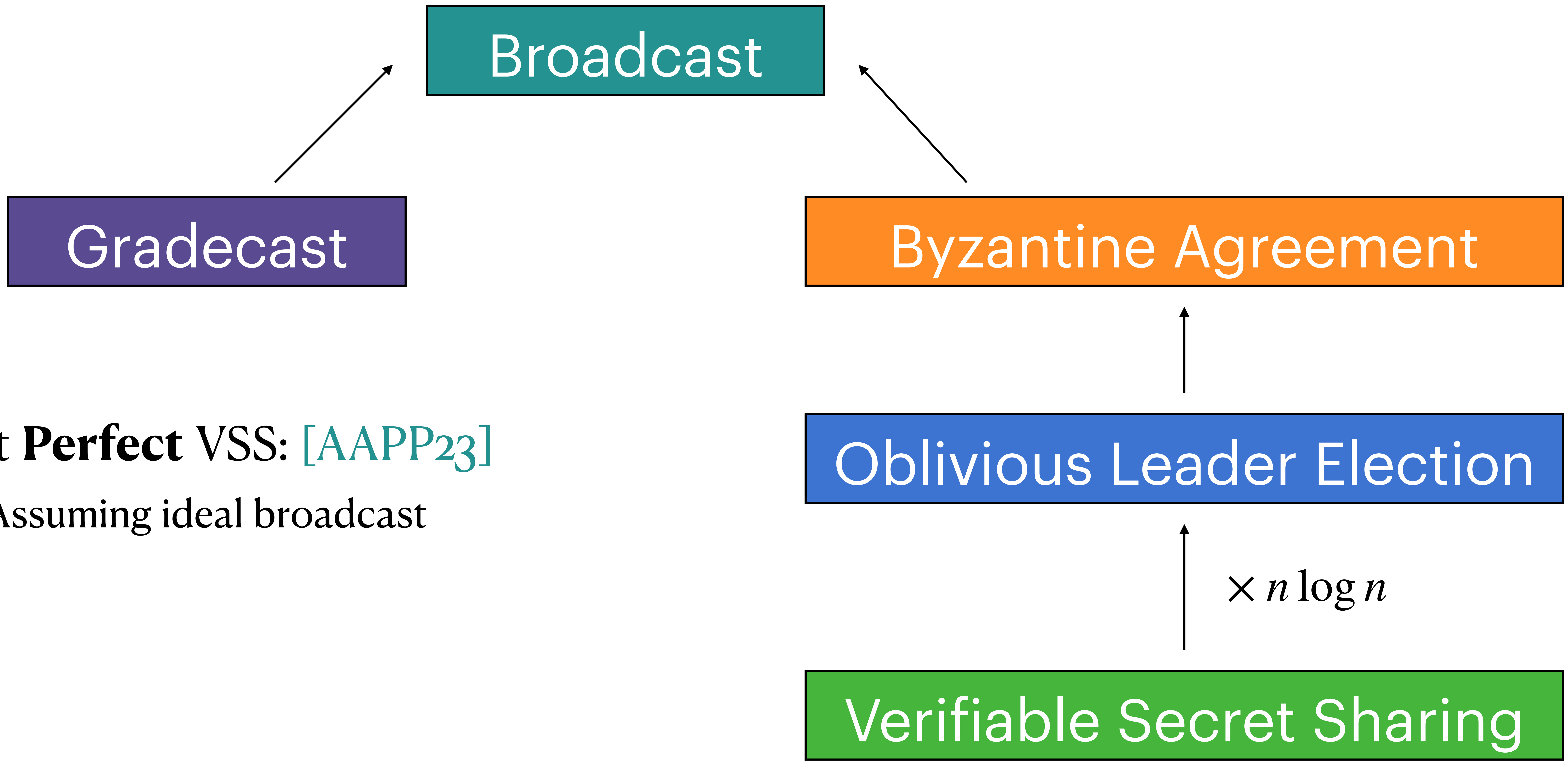


[KK06] Framework



Best **Perfect** VSS: [AAPP23]

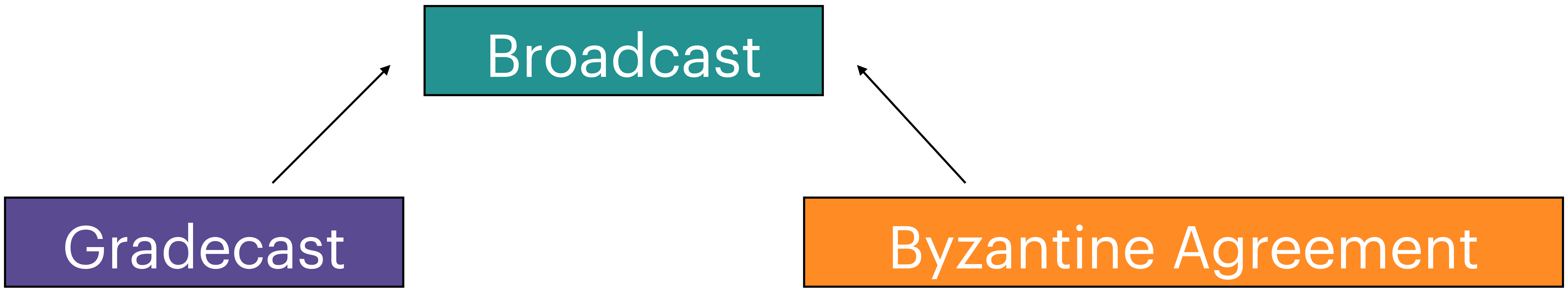
[KK06] Framework



Best **Perfect** VSS: [AAPP23]

Assuming ideal broadcast

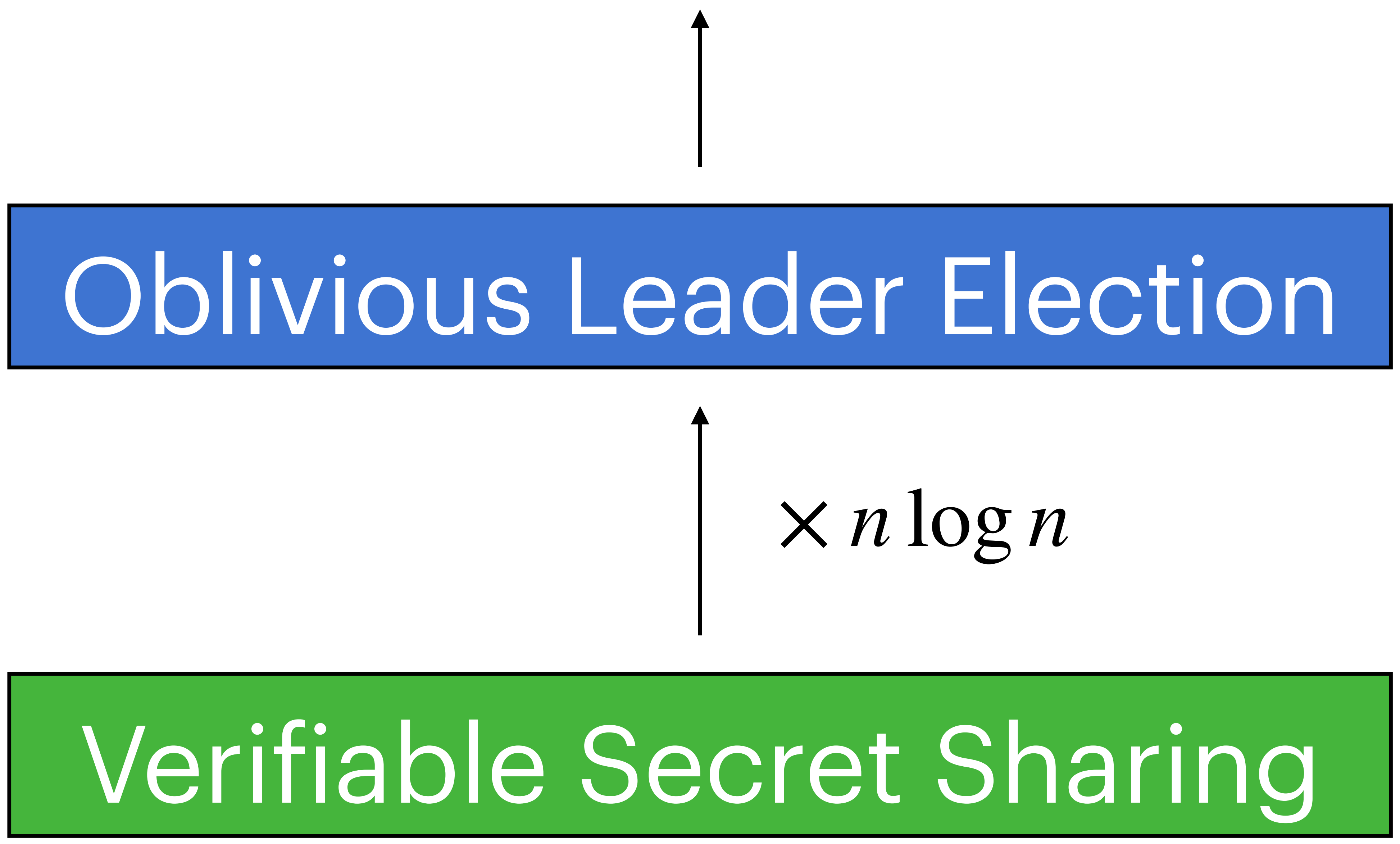
[KK06] Framework



Best **Perfect** VSS: [AAPP23]

Assuming ideal broadcast

$\tilde{O}(mn + n^3)$ for m secrets



[KK06] Framework

Broadcast

Gradecast

Byzantine Agreement

Oblivious Leader Election

$\times n \log n$

Verifiable Secret Sharing

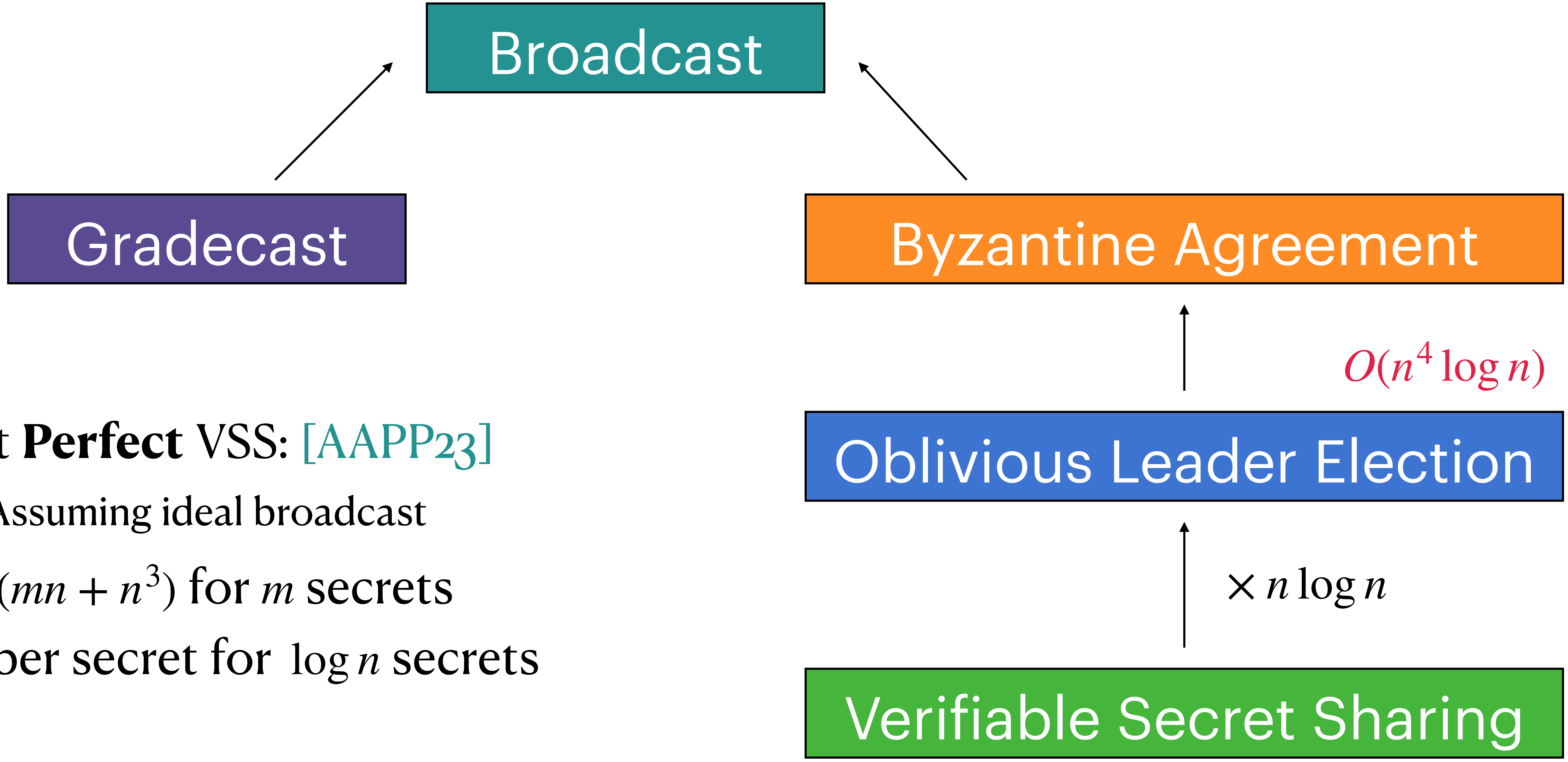
Best **Perfect** VSS: [AAPP23]

Assuming ideal broadcast

$\tilde{O}(mn + n^3)$ for m secrets

$O(n^3)$ per secret for $\log n$ secrets

[KK06] Framework



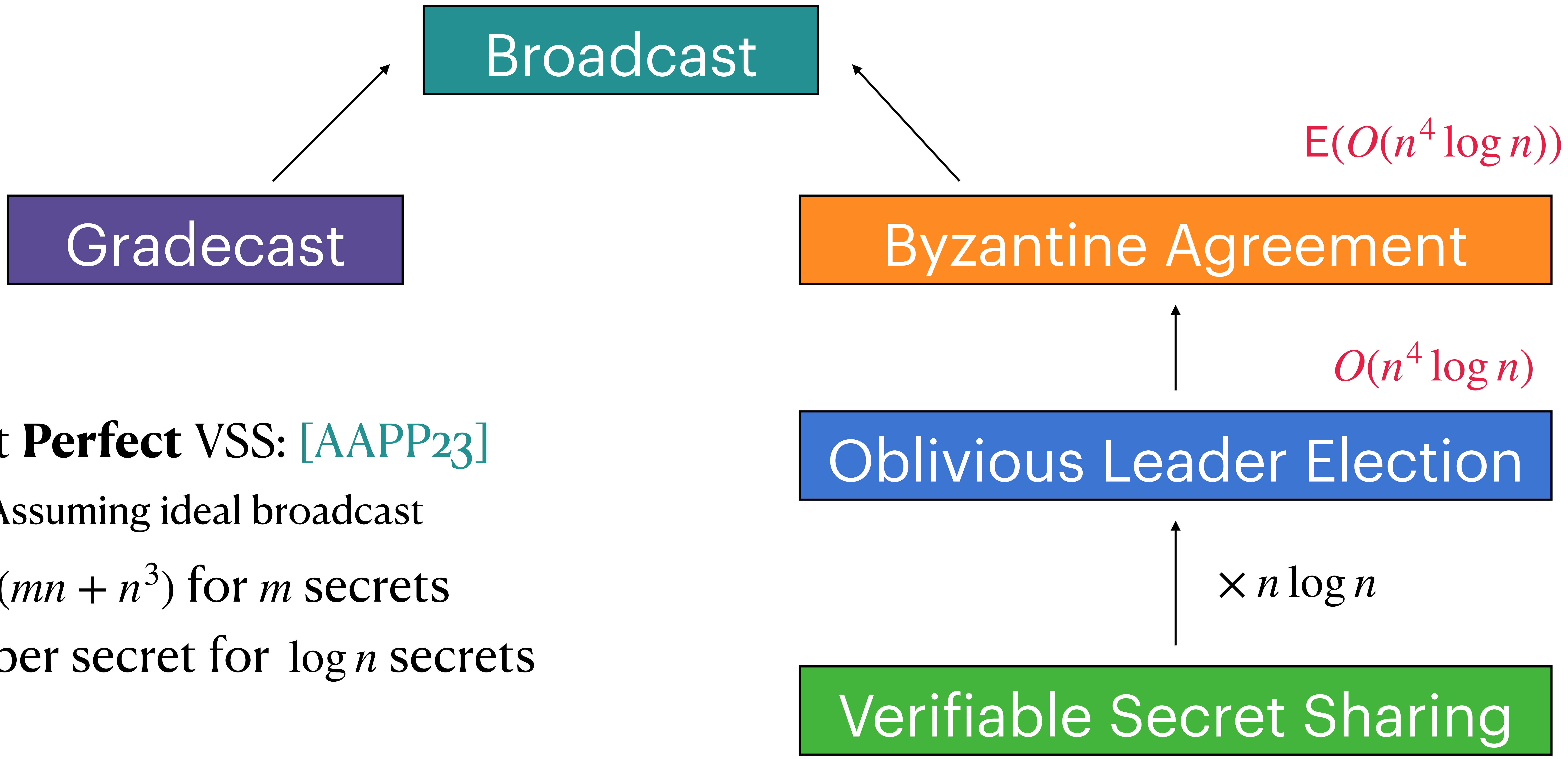
Best **Perfect** VSS: [AAPP23]

Assuming ideal broadcast

$\tilde{O}(mn + n^3)$ for m secrets

$O(n^3)$ per secret for $\log n$ secrets

[KK06] Framework



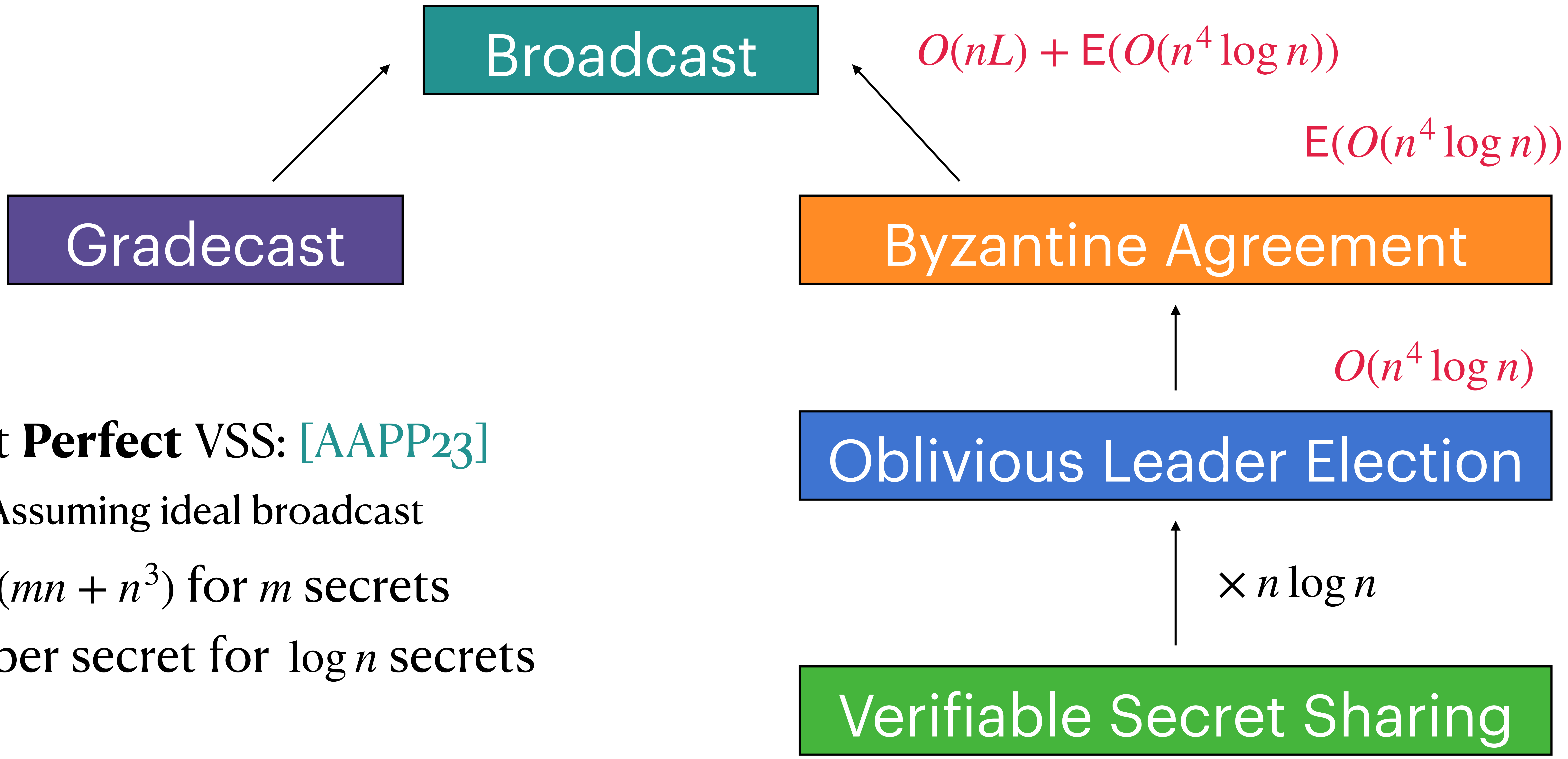
Best **Perfect** VSS: [AAPP23]

Assuming ideal broadcast

$\tilde{O}(mn + n^3)$ for m secrets

$O(n^3)$ per secret for $\log n$ secrets

[KK06] Framework



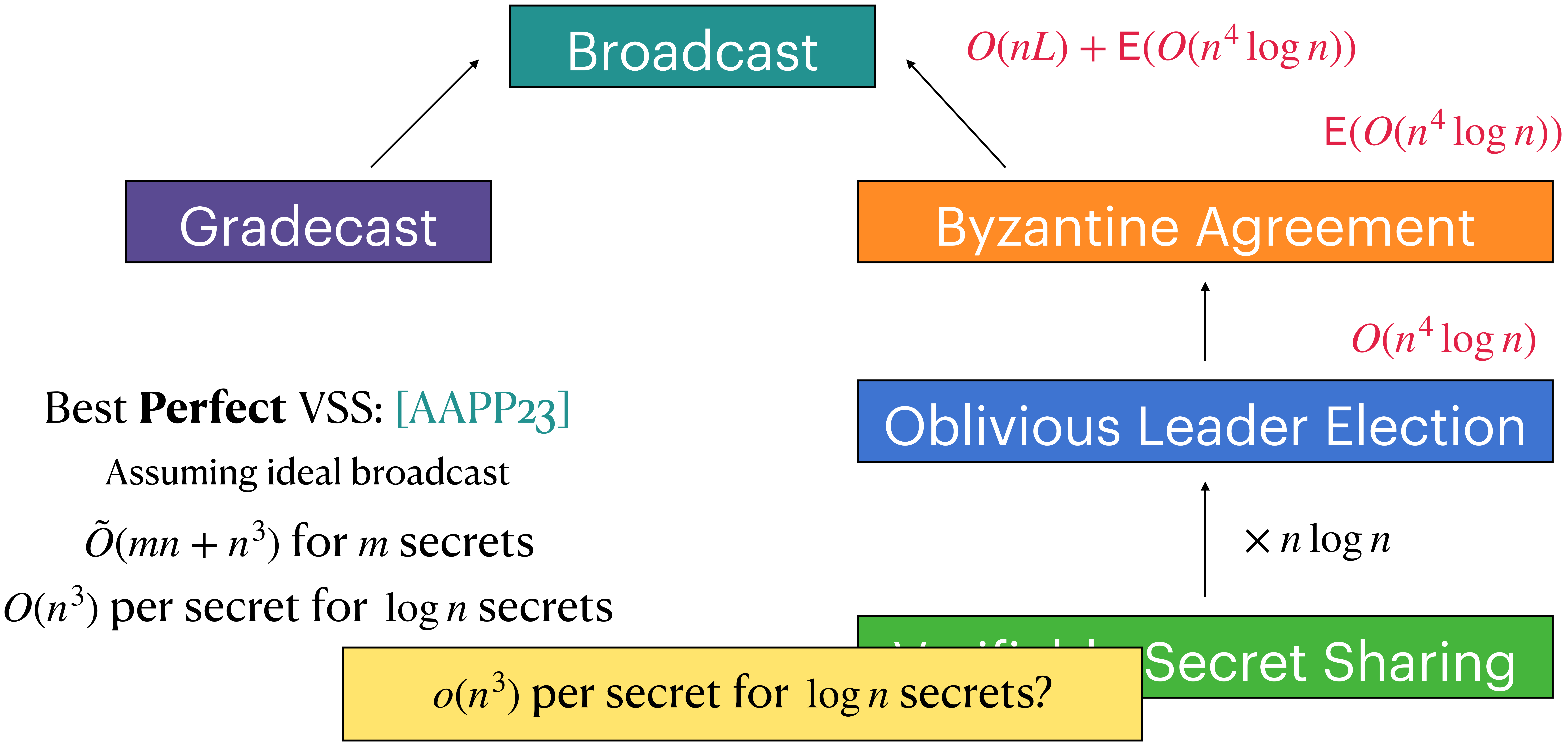
Best **Perfect** VSS: [AAPP23]

Assuming ideal broadcast

$\tilde{O}(mn + n^3)$ for m secrets

$O(n^3)$ per secret for $\log n$ secrets

[KK06] Framework



We're not done yet!

Why Perfect?

Why Perfect?

$$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader } \textbf{OR} \text{ the VSS fails}] \leq \frac{1}{2}$$

Why Perfect?

$$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader } \textbf{OR} \text{ the VSS fails}] \leq \frac{1}{2}$$

$$\Pr[\text{Everyone agrees on honest leader}] \geq \frac{1}{2}$$

Why Perfect?

$$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader } \textbf{OR} \text{ the VSS fails}] \leq \frac{1}{2}$$

$$\Pr[\text{Everyone agrees on honest leader}] \geq \frac{1}{2}$$

Best Perfect VSS for m secrets: [AAPP23]

$\tilde{O}(mn + n^3)$

Why Perfect?

$$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader } \textbf{OR} \text{ the VSS fails}] \leq \frac{1}{2}$$

$$\Pr[\text{Everyone agrees on honest leader}] \geq \frac{1}{2}$$

Best Perfect VSS for m secrets: [AAPP23]

$\tilde{O}(mn + n^3)$

Our statistical VSS for m secrets with error ϵ

$\tilde{O}(mn^2 + n^2 \log(n/\epsilon))$

Why Perfect?

$$\Pr[\text{No agreement } \textbf{OR} \text{ corrupted leader } \textbf{OR} \text{ the VSS fails}] \leq \frac{1}{2}$$

$$\Pr[\text{Everyone agrees on honest leader}] \geq \frac{1}{2}$$

Best Perfect VSS for m secrets: [AAPP23]

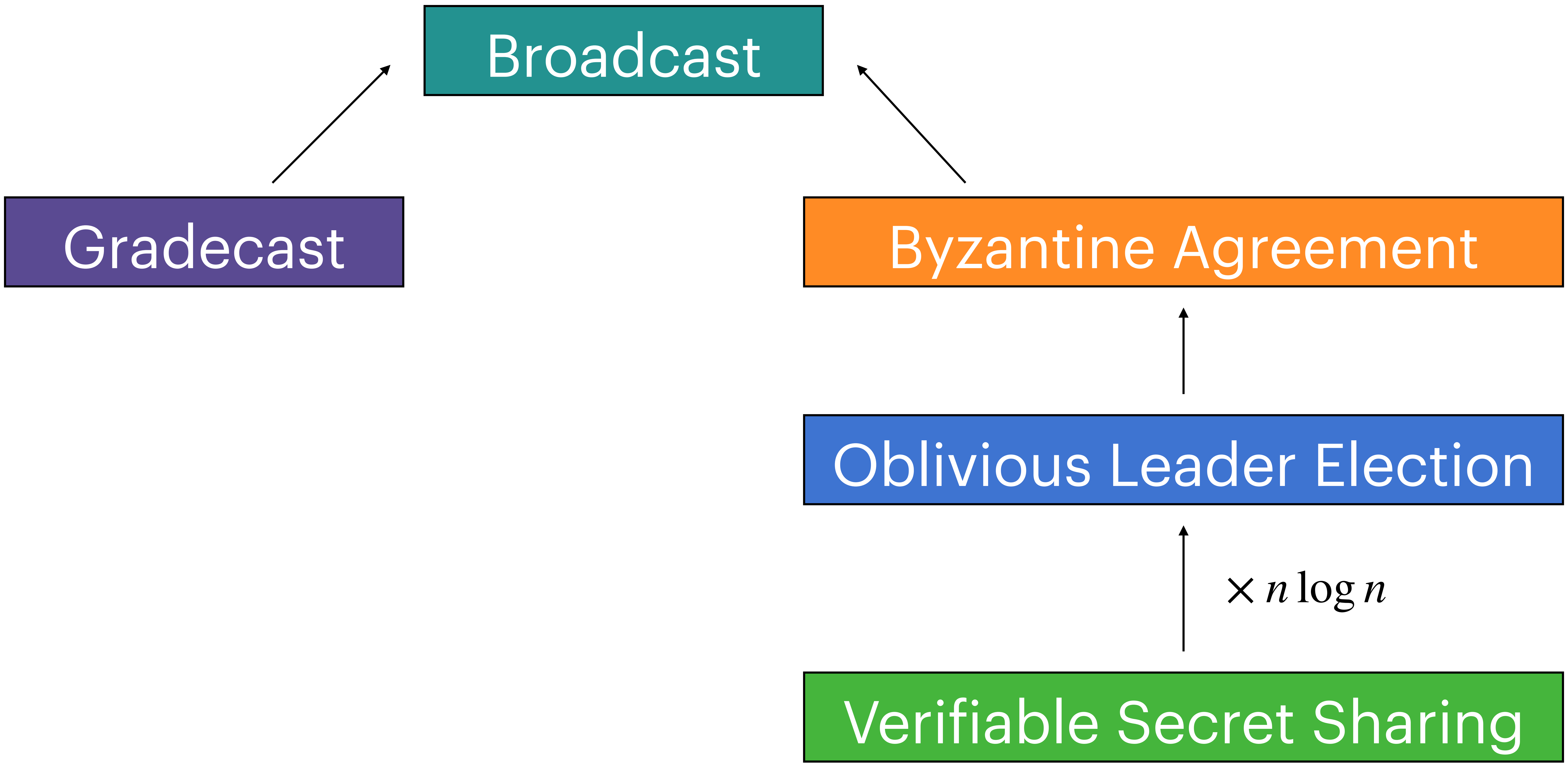
$\tilde{O}(mn + n^3)$

Our statistical VSS for m secrets with error ϵ

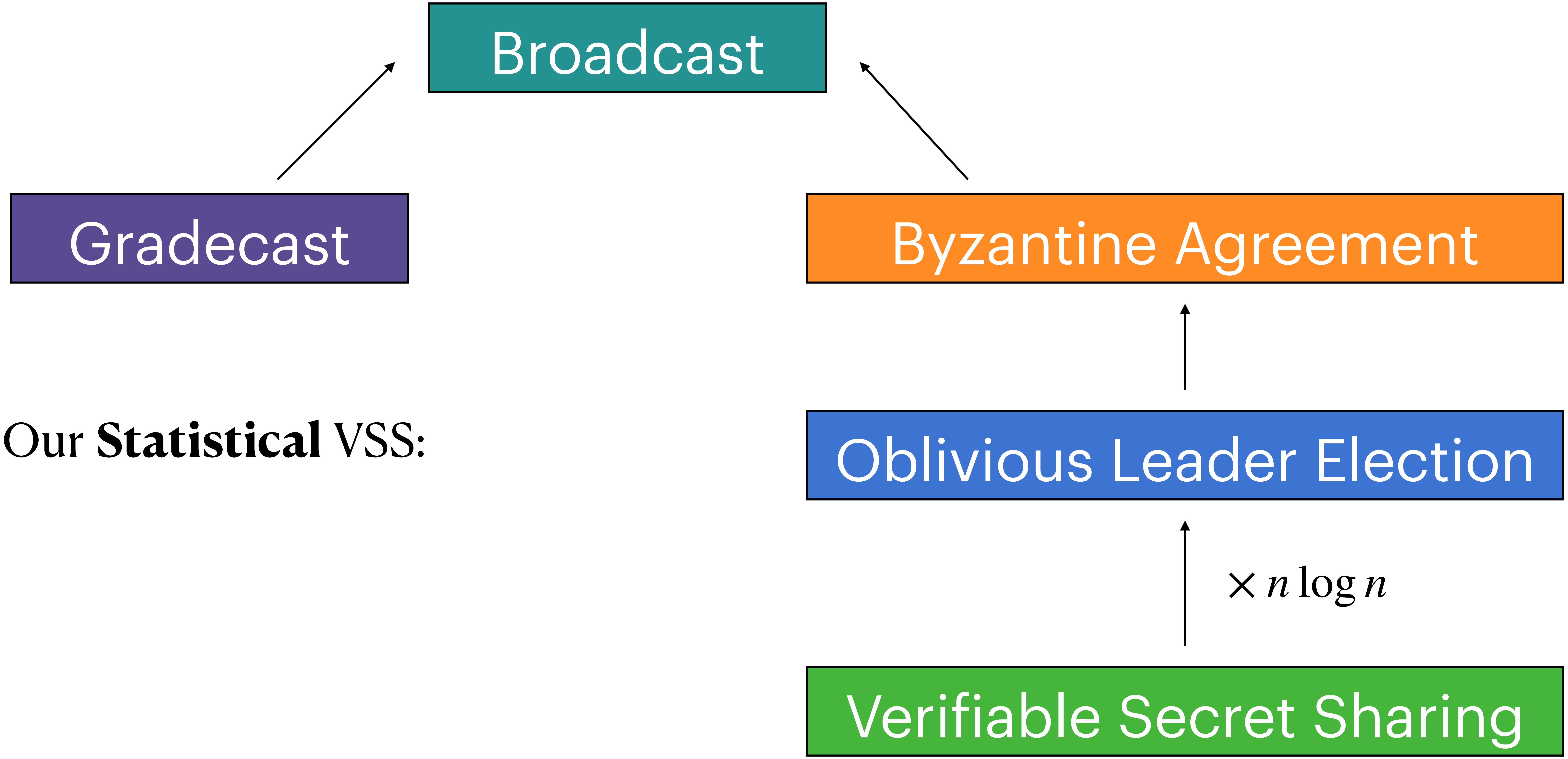
$\tilde{O}(mn^2 + n^2 \log(n/\epsilon))$

$$\epsilon = \frac{1}{\text{poly } n} \text{ suffices!}$$

[KK06] Framework

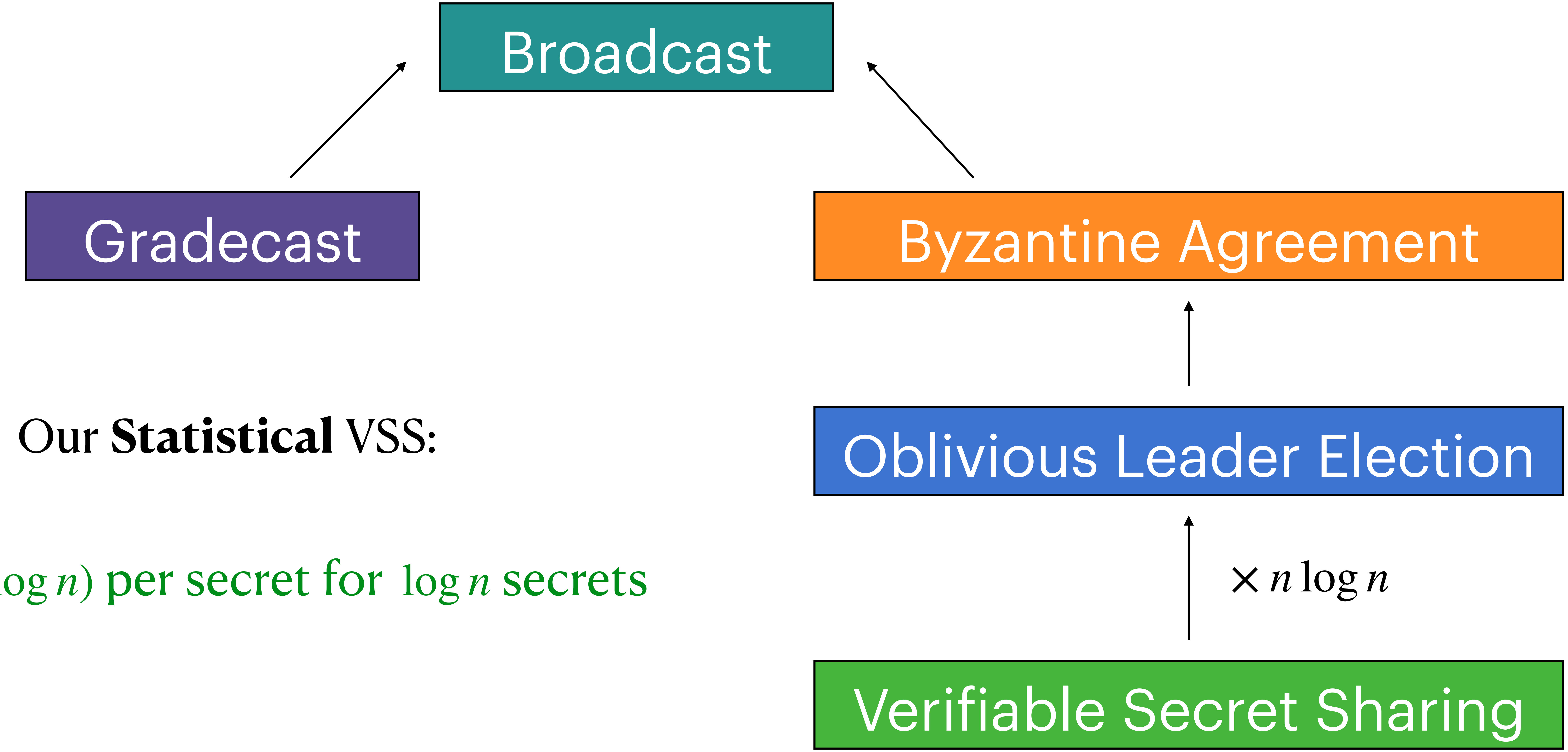


[KK06] Framework



Our **Statistical** VSS:

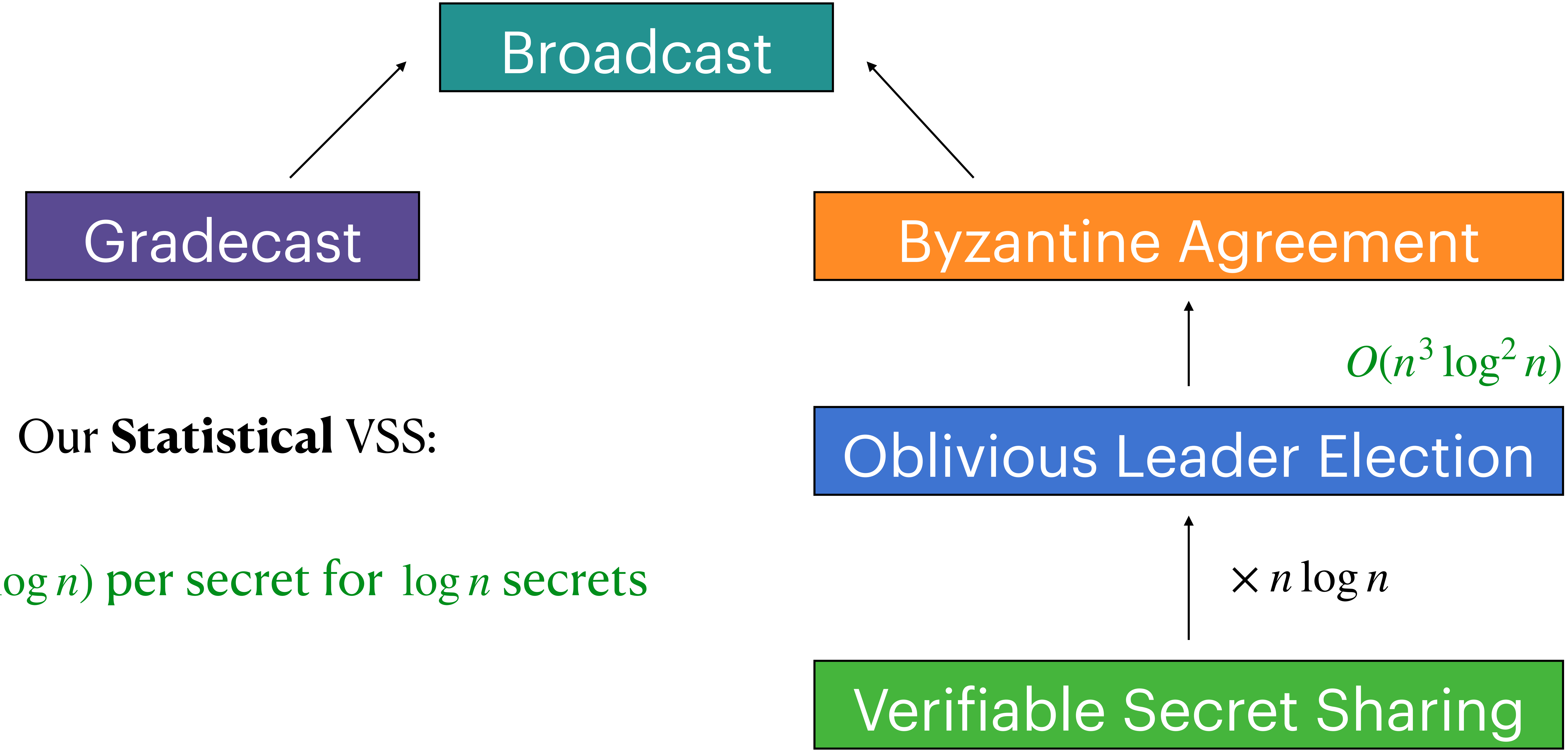
[KK06] Framework



Our **Statistical** VSS:

$O(n^2 \log n)$ per secret for $\log n$ secrets

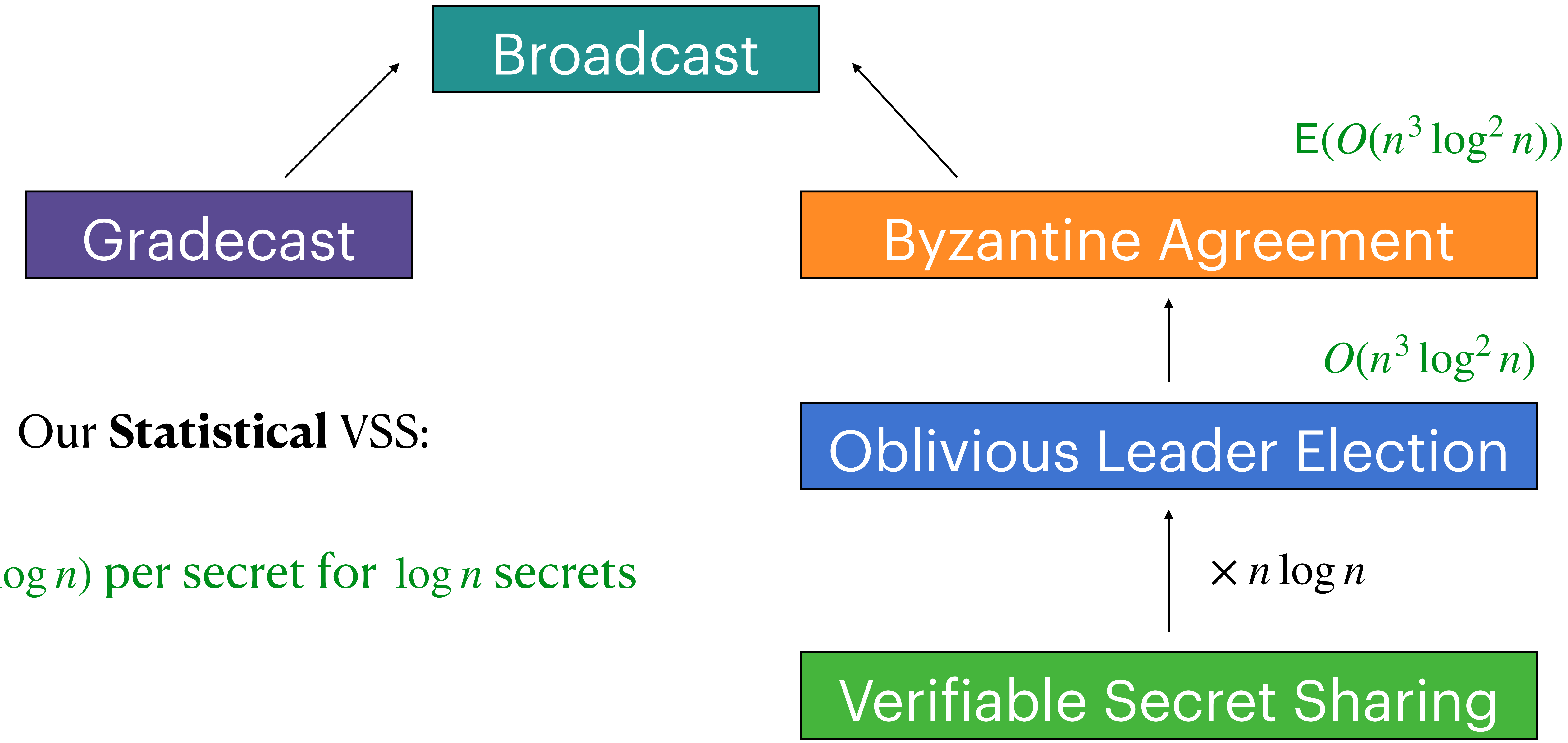
[KK06] Framework



Our **Statistical** VSS:

$O(n^2 \log n)$ per secret for $\log n$ secrets

[KK06] Framework



Our **Statistical** VSS:

$O(n^2 \log n)$ per secret for $\log n$ secrets

[KK06] Framework

Broadcast

$O(nL) + \mathsf{E}(O(n^3 \log^2 n))$

Gradecast

$\mathsf{E}(O(n^3 \log^2 n))$

Byzantine Agreement

$O(n^3 \log^2 n)$

Oblivious Leader Election

Our **Statistical** VSS:

$\times\, n \log n$

$O(n^2 \log n)$ per secret for $\log n$ secrets

Verifiable Secret Sharing

Contributions

- **Conceptual contributions:**
  - Statistical OLE suffices
  - OLE from statistical VSS
- **Technical contributions:**
  - Statistical OLE with lesser secrets
  - Amortized Statistical VSS for lesser secrets

Conclusions

	Communication	Rounds	
Perfect Broadcast	$O(nL) + \mathsf{E}(O(n^3 \log^2 n))$	$\mathsf{E}(O(1))$	Optimal for $L \geq n^2 \log^2 n$
Perfect (Parallel) Broadcast	$O(n^2L) + \mathsf{E}(O(n^3 \log^2 n))$	$\mathsf{E}(O(1))$	Optimal for $L \geq n \log^2 n$
Statistical VSS	$O(n^2 \log n)$ per secret for $O(\log n)$ secrets	$O(1)$	

Statistical OLE $\Longrightarrow$ Perfect broadcast in constant expected time

Conclusions

	Communication	Rounds	
Perfect Broadcast	$O(nL) + \mathsf{E}(O(n^3 \log^2 n))$	$\mathsf{E}(O(1))$	Optimal for $L \geq n^2 \log^2 n$
Perfect (Parallel) Broadcast	$O(n^2 L) + \mathsf{E}(O(n^3 \log^2 n))$	$\mathsf{E}(O(1))$	Optimal for $L \geq n \log^2 n$
Statistical VSS	$O(n^2 \log n)$ per secret for $O(\log n)$ secrets	$O(1)$	

Statistical OLE $\Longrightarrow$ Perfect broadcast in constant expected time

Thank you!