Asymptotically Free Broadcast in Constant Expected Time via Packed VSS

Gilad Asharov
Bar-Ilan University

Ittai Abraham
VMWare Research

Shravani Patil
IISC Bangalore

Arpita Patra
IISC Bangalore

Broadcast for perfect MPC is essentially free*!

Broadcast for perfect MPC is essentially free*!

Settings

- Perfect:
  - Computationally unbounded adversary
  - Zero-probability of error
- Optimal resilience: $t < n/3$

BenOr, Goldwasser, Wigderson 88:

BenOr, Goldwasser, Wigderson 88:

P_1	P_2	P_{n-1}	P_n
x_1	x_2	x_{n-1}	x_n
VSS	VSS	VSS	VSS

VSS $= O(n^2)$ **p2p** + $O(n^2)$ **broadcast**

Constant round

BenOr, Goldwasser, Wigderson 88:

P_1	P_2	P_{n-1}	P_n
x_1	x_2	x_{n-1}	x_n
VSS	VSS	VSS	VSS

VSS = $O(n^2)$ **p2p** + $O(n^2)$ **broadcast**

Constant round

BenOr, Goldwasser, Wigderson 88:

P_1 P_2 P_{n-1} P_n

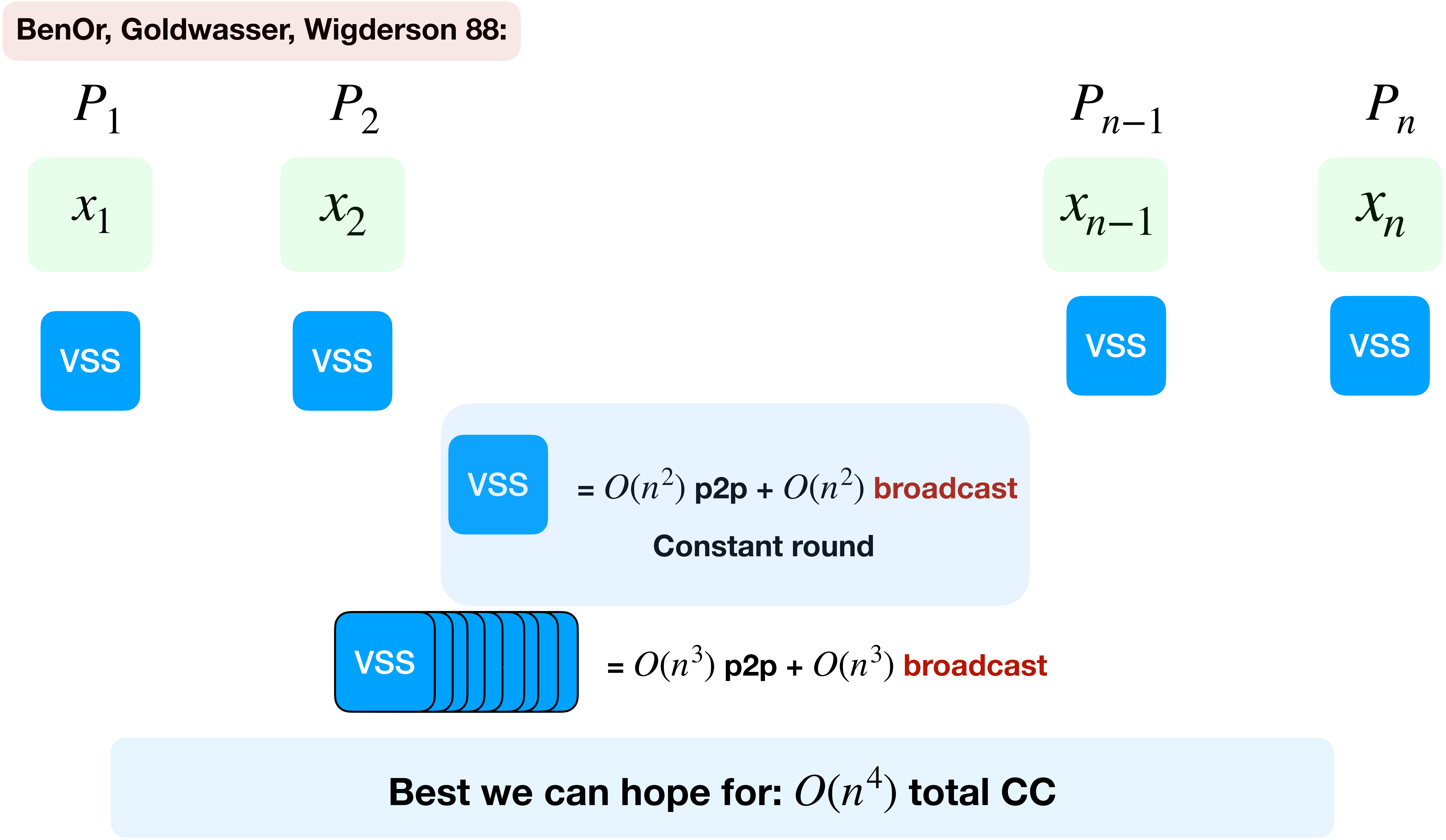
x_1 x_2 x_{n-1} x_n

VSS VSS VSS VSS

VSS = $O(n^2)$ **p2p** + $O(n^2)$ **broadcast**

Constant round

VSS = $O(n^3)$ **p2p** + $O(n^3)$ **broadcast**



BenOr, Goldwasser, Wigderson 88:
P_1
P_2
P_{n-1}
P_n
x_1
x_2
x_{n-1}
x_n
VSS
VSS
VSS
VSS
VSS
= $O(n^2)$ p2p + $O(n^2)$ broadcast
Constant round
VSS
= $O(n^3)$ p2p + $O(n^3)$ broadcast
Best we can hope for: $O(n^4)$ total CC

BenOr, Goldwasser, Wigderson 88:

P_1	P_2	P_{n-1}	P_n
x_1	x_2	x_{n-1}	x_n
VSS	VSS	VSS	VSS

VSS = $O(n^2)$ **p2p** + $O(n^2)$ **broadcast**

Constant round

VSS = $O(n^3)$ **p2p** + $O(n^3)$ **broadcast**

Best we can hope for: $O(n^4)$ total CC

$$n \times \mathrm{BC}(n^2)$$

State of the Art: $n \times \mathrm{BC}(n^2)$

for simplicity, counting "words" and not "bits" -> i.e., ignoring $\log n$ factor

Communication Complexity p2p

Round Complexity

State of the Art: $n \times \mathrm{BC}(n^2)$

for simplicity, counting "words" and not "bits" -> i.e., ignoring $\log n$ factor

	Efficient but slow	Fast but inefficient
	[CW89,BGP91,Che21]	[FM88,KK06]
Communication Complexity p2p		
Round Complexity		

State of the Art: $n \times \mathrm{BC}(n^2)$

for simplicity, counting "words" and not "bits" -> i.e., ignoring $\log n$ factor

	Efficient but slow	Fast but inefficient
	[CW89,BGP91,Che21]	[FM88,KK06]
Communication Complexity p2p	$O(n^4)$	
Round Complexity		

State of the Art: $n \times \text{BC}(n^2)$

for simplicity, counting "words" and not "bits" -> i.e., ignoring $\log n$ factor

	Efficient but slow	Fast but inefficient
	[CW89,BGP91,Che21]	[FM88,KK06]
Communication Complexity p2p	$O(n^4)$	
Round Complexity	$\Theta(n)$	

State of the Art: $n \times \mathrm{BC}(n^2)$

for simplicity, counting "words" and not "bits" -> i.e., ignoring $\log n$ factor

	Efficient but slow	Fast but inefficient
	[CW89,BGP91,Che21]	[FM88,KK06]
Communication Complexity p2p	$O(n^4)$	
Round Complexity	$\Theta(n)$	Expected $O(1)$

State of the Art: $n \times \mathrm{BC}(n^2)$

for simplicity, counting "words" and not "bits" -> i.e., ignoring $\log n$ factor

	Efficient but slow	Fast but inefficient
	[CW89,BGP91,Che21]	[FM88,KK06]
Communication Complexity p2p	$O(n^4)$	$O(n^6)$
Round Complexity	$\Theta(n)$	Expected $O(1)$

State of the Art: $n \times \mathrm{BC}(n^2)$

for simplicity, counting "words" and not "bits" -> i.e., ignoring $\log n$ factor

Strict $O(1)$ rounds is impossible to achieve

[FL82] For any protocol, there exists an execution that requires $t+1$ rounds

	Efficient but slow	Fast but inefficient
	[CW89,BGP91,Che21]	[FM88,KK06]
Communication Complexity p2p	$O(n^4)$	$O(n^6)$
Round Complexity	$\Theta(n)$	**Expected** $O(1)$

State of the Art: $n \times \text{BC}(n^2)$

for simplicity, counting "words" and not "bits" -> i.e., ignoring $\log n$ factor

Strict $O(1)$ rounds is impossible to achieve

[FL82] For any protocol, there exists an execution that requires $t+1$ rounds

		Efficient but slow	Fast but inefficient
		[CW89,BGP91,Che21]	[FM88,KK06]
Communication Complexity p2p	$n \times \text{BC}(n^2)$	$O(n^4)$	$O(n^6)$
	$1 \times \text{BC}(L)$	$O(nL + n^2)$	$O(n^2L + n^6)$
Round Complexity		$\Theta(n)$	Expected $O(1)$

A circuit with depth 10 and
$n = 300$ participants

Instead of $\approx$ 10 rounds
we have $\approx$ 3000 rounds

		Efficient but slow [CW89,BGP91,Che21]	Fast but inefficient [FM88,KK06]
Communication Complexity p2p	$n \times \mathrm{BC}(n^2)$	$O(n^4)$	$O(n^6)$
	$1 \times \mathrm{BC}(L)$	$O(nL + n^2)$	$O(n^2L + n^6)$
Round Complexity		$\Theta(n)$	**Expected** $O(1)$

A circuit with depth 10 and $n = 300$ participants

Instead of $\approx$ 10 rounds we have $\approx$ 3000 rounds

For $n = 300$, $n^3 \approx 27\text{MB}$ $n^5 \approx 2.4$ terabytes!

		Efficient but slow	Fast but inefficient
		[CW89,BGP91,Che21]	[FM88,KK06]
Communication Complexity	$n \times \mathrm{BC}(n^2)$	$O(n^4)$	$O(n^6)$
p2p	$1 \times \mathrm{BC}(L)$	$O(nL + n^2)$	$O(n^2L + n^6)$
Round Complexity		$\Theta(n)$	Expected $O(1)$

Goal: Better Broadcast

Main Result

- Parallel broadcast protocol with perfect security and optimal resilience ($t < n/3$)

Main Result

- Parallel broadcast protocol with perfect security and optimal resilience ($t < n/3$)
  - $n \times \mathrm{BC}(L)$: n senders, each broadcasting a message of size L

Main Result

- Parallel broadcast protocol with perfect security and optimal resilience ($t < n/3$)
  - $n \times \text{BC}(L)$: n senders, each broadcasting a message of size L

Best we can hope for:
$O(n^2L)$ + expected $O(1)$ round

Main Result

- Parallel broadcast protocol with perfect security and optimal resilience ($t < n/3$)
  - $n \times \text{BC}(L)$: n senders, each broadcasting a message of size L
  - $O(n^2L + n^4)$ communication complexity

Best we can hope for:
$O(n^2L)$ + expected $O(1)$ round

Main Result

- Parallel broadcast protocol with perfect security and optimal resilience ($t < n/3$)
  - $n \times \text{BC}(L)$: n senders, each broadcasting a message of size L
  - $O(n^2L + n^4)$ communication complexity
  - Expected $O(1)$ rounds

Best we can hope for:
$O(n^2L)$ + expected $O(1)$ round

Main Result

- Parallel broadcast protocol with perfect security and optimal resilience ($t < n/3$)
  - $n \times \text{BC}(L)$: n senders, each broadcasting a message of size L
  - $O(n^2L + n^4)$ communication complexity
  - Expected $O(1)$ rounds

Best we can hope for: $O(n^2L)$ + expected $O(1)$ round

The protocol is balanced!

Main Result

- Parallel broadcast protocol with perfect security and optimal resilience ($t < n/3$)
  - $n \times \text{BC}(L)$: n senders, each broadcasting a message of size L
  - $O(n^2L + n^4)$ communication complexity
  - Expected $O(1)$ rounds

Best we can hope for:
$O(n^2L)$ + expected $O(1)$ round

The protocol is balanced!

$n \times \text{BC}(n^2)$ **is essentially free!**

Main Result

- Parallel broadcast protocol with perfect security and optimal resilience ($t < n/3$)
  - $n \times \text{BC}(L)$: n senders, each broadcasting a message of size L
  - $O(n^2L + n^4)$ communication complexity
  - Expected $O(1)$ rounds

Best we can hope for: $O(n^2L)$ + expected $O(1)$ round

The protocol is balanced!

$n \times \text{BC}(n^2)$ **is essentially free!**

$1 \times \text{BC}(L)$: $O(nL + n^4)$ **communication + expected** $O(1)$ **rounds**

$$n = 300$$

	Total CC of	Each party sends/receives	Over 1gbps
Before	$O(n^6)$		
Ours	$O(n^4)$		

$$n = 300$$

	Total CC of	Each party sends/receives	Over 1gbps
Before	$O(n^6)$	$n^5 \approx 2.4$ terabytes	
Ours	$O(n^4)$		

$$n = 300$$

	Total CC of	Each party sends/receives	Over 1gbps
Before	$O(n^6)$	$n^5 \approx 2.4$ terabytes	5.3 hours
Ours	$O(n^4)$		

$$n = 300$$

	Total CC of	Each party sends/receives	Over 1gbps
Before	$O(n^6)$	$n^5 \approx 2.4$ terabytes	5.3 hours
Ours	$O(n^4)$	$n^3 \approx 27$ MB	

$$n = 300$$

	Total CC of	Each party sends/receives	Over 1gbps
Before	$O(n^6)$	$n^5 \approx 2.4$ terabytes	5.3 hours
Ours	$O(n^4)$	$n^3 \approx 27$ MB	200 ms

$$n = 300$$

	Total CC of	Each party sends/receives	Over 1gbps
Before	$O(n^6)$	$n^5 \approx 2.4$ terabytes	5.3 hours
Ours	$O(n^4)$	$n^3 \approx 27$ MB	200 ms

x90,000 improvement

Perfect MPC in the Broadcast-Hybrid Model

For constant depth circuit		Efficient but slow	Fast but inefficient
		[HMP00, BTH08, GLS19]	[BGW88, CCD88, GRR98, CDM00, **A**LR11, A**A**Y21]
Communication Complexity	**p2p**		
	Broadcast		
Round Complexity			

Perfect MPC in the Broadcast-Hybrid Model

STOC Test of Time Award!

For constant depth circuit		Efficient but slow	Fast but ineffici…
		[HMP00, BTH08, GLS19]	[BGW88, CCD88, GRR98, CDM00, **A**LR11, A**A**Y21]
Communication Complexity	p2p		
	Broadcast		
Round Complexity			

TCC Test of Time Award!

…ct MPC in the Broadcast-Hybrid Model

STOC Test of Time Award!

For constant depth circuit

		Efficient but slow	Fast but ineffici…
		[HMP00, BTH08, GLS19]	[BGW88, CCD88, GRR98, CDM00, **A**LR11, A**A**Y21]
Communication Complexity	p2p		
	Broadcast		
Round Complexity			

…ct MPC in the Broadcast-Hybrid Model

TCC Test of Time Award!

STOC Test of Time Award!

For constant depth circuit		Efficient but slow [HMP00, BTH08, GLS19]	Fast but ineffici… [BGW88, CCD88, GRR98, CDM00, **A**LR11, A**A**Y21]
Communication Complexity	**p2p**	$O(\|C\|n + n^3)$	
	Broadcast	$O(n \log n)$	
Round Complexity			

TCC Test of Time Award!

ct MPC in the Broadcast-Hybrid Model

STOC Test of Time Award!

For constant depth circuit

		Efficient but slow	Fast but ineffici
		[HMP00, BTH08, GLS19]	[BGW88, CCD88, GRR98, CDM00, **A**LR11, A**A**Y21]
Communication Complexity	**p2p**	$O(\|C\|n + n^3)$	
	Broadcast	$O(n \log n)$	
Round Complexity		$O(n)$	

Due to "player elimination"

TCC Test of Time Award!

…ct MPC in the Broadcast-Hybrid Model

STOC Test of Time Award!

For constant depth circuit

		Efficient but slow	Fast but inefficie…
		[HMP00, BTH08, GLS19]	[BGW88, CCD88, GRR98, CDM00, **A**LR11, A**A**Y21]
Communication Complexity	**p2p**	$O(\|C\|n + n^3)$	
	Broadcast	$O(n \log n)$	
Round Complexity		$O(n)$	$O(1)$

Due to "player elimination"

…ct MPC in the Broadcast-Hybrid Model

TCC Test of Time Award!

STOC Test of Time Award!

For constant depth circuit

		Efficient but slow	Fast but ineffici…
		[HMP00, BTH08, GLS19]	[BGW88, CCD88, GRR98, CDM00, **A**LR11, A**A**Y21]
Communication Complexity	**p2p**	$O(\|C\|n + n^3)$	$O(\|C\|n^3)$
	Broadcast	$O(n \log n)$	$O(\|C\|n^3)$
Round Complexity		$O(n)$	$O(1)$

Due to “player elimination”

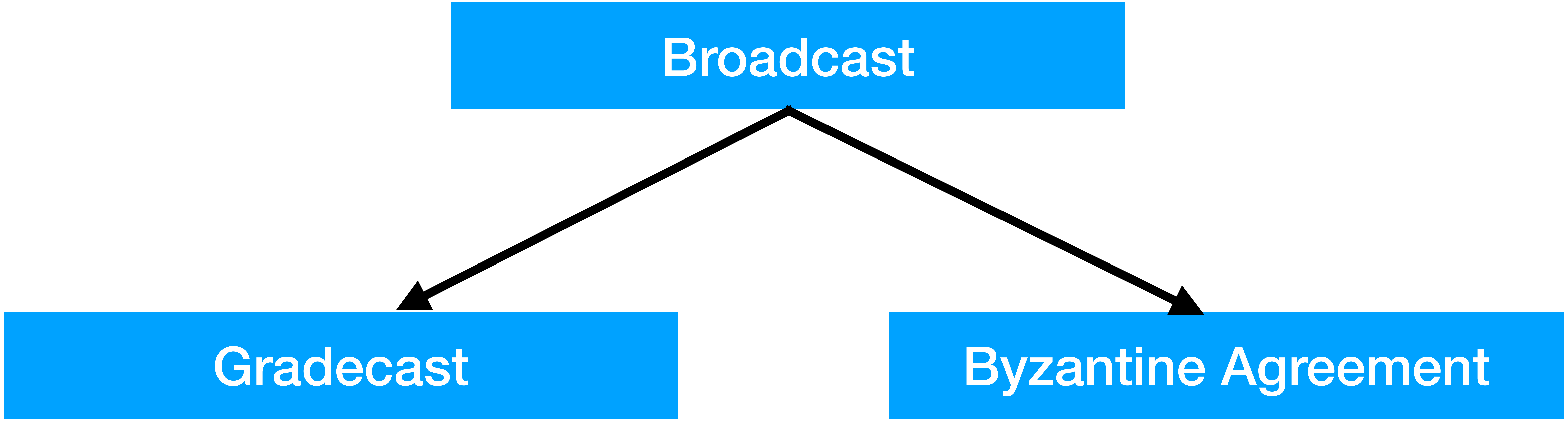

MPC:
Efficient but slow
Efficient but slow
Fast but inefficient
+
+
+
Broadcast:
Efficient but slow
Fast but inefficient
Fast but inefficient
Very Slow MPC
Slow and inefficient MPC
Very inefficient MPC

MPC:	Efficient but slow	Efficient but slow	Fast but inefficient
	+	+	+
Broadcast:	Efficient but slow	Fast but inefficient	Fast but inefficient
	Very Slow MPC	Slow and inefficient MPC	Very inefficient MPC
Communication Complexity	$O(\lvert C \rvert n + n^3)$	$O(\lvert C \rvert n + n^7)$	$O(\lvert C \rvert n^6)$
Round Complexity	$O(n^2)$	$O(n)$ **Expected**	$O(1)$ **Expected**

MPC:	Efficient but slow	Efficient but slow	Fast but inefficient
	+	+	+
Broadcast:	Efficient but slow	Our Broadcast	Our Broadcast
	Very Slow MPC	Slow and inefficient MPC	Very inefficient MPC
Communication Complexity	$O(\lvert C \rvert n + n^3)$	$O(\lvert C \rvert n + n^5)$ $O(\lvert C \rvert n + n^7)$	$O(\lvert C \rvert n^4)$ $O(\lvert C \rvert n^6)$
Round Complexity	$O(n^2)$	$O(n)$ Expected	$O(1)$ Expected

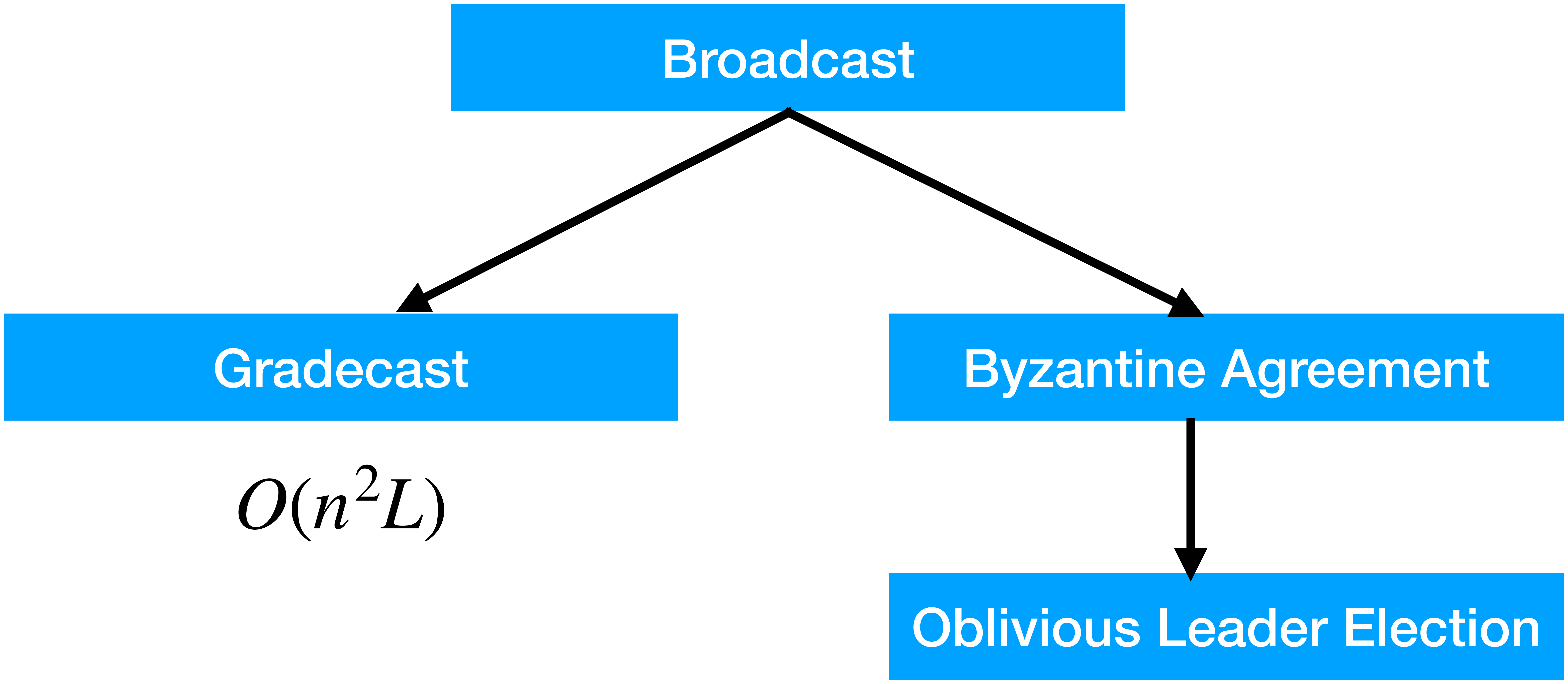
MPC:	Efficient but slow	Efficient but slow	Fast but inefficient	Coming up!
	+	+	+	+
Broadcast:	Efficient but slow	Our Broadcast	Our Broadcast	Our Broadcast
	Very Slow MPC	Slow and inefficient MPC	Very inefficient MPC	
Communication Complexity	$O(\|C\|n + n^3)$	$O(\|C\|n + n^5)$ $O(\|C\|n + n^7)$	$O(\|C\|n^4)$ $O(\|C\|n^6)$	$O(\|C\|n + n^4)$
Round Complexity	$O(n^2)$	$O(n)$ **Expected**	$O(1)$ **Expected**	$O(1)$ **Expected**
				In submission

Structure of Katz and Koo

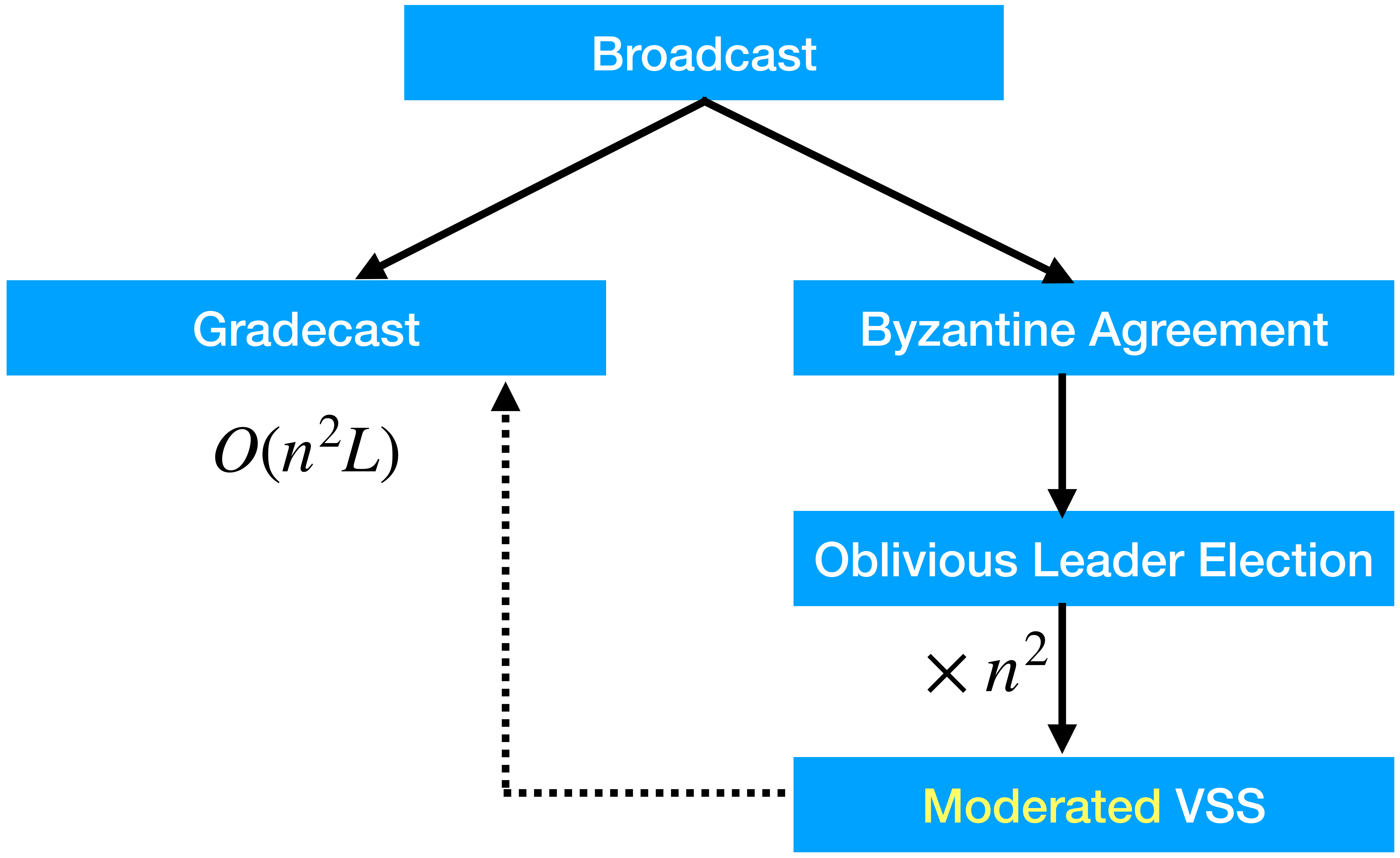


$$O(n^2L)$$

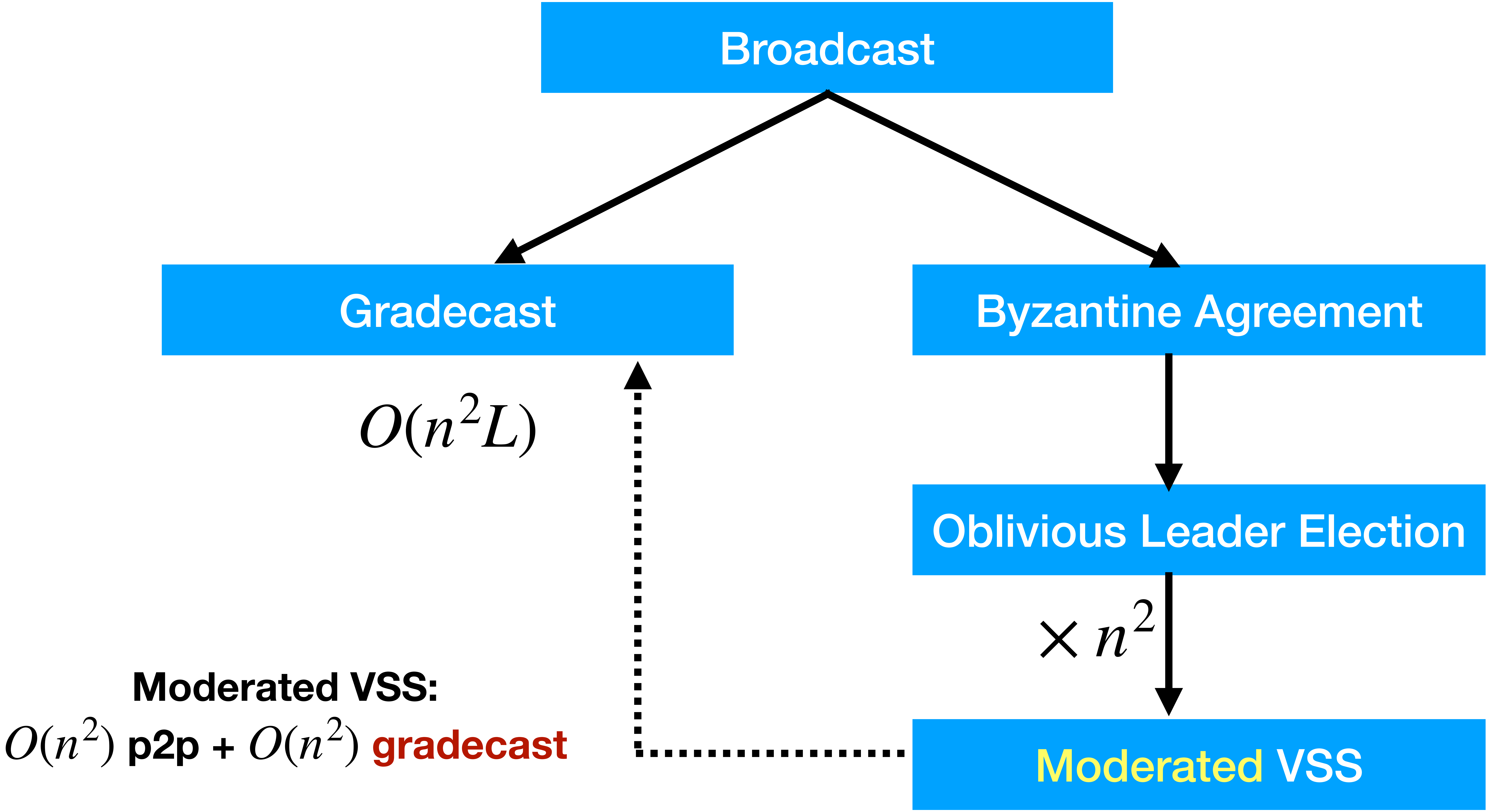
Structure of Katz and Koo



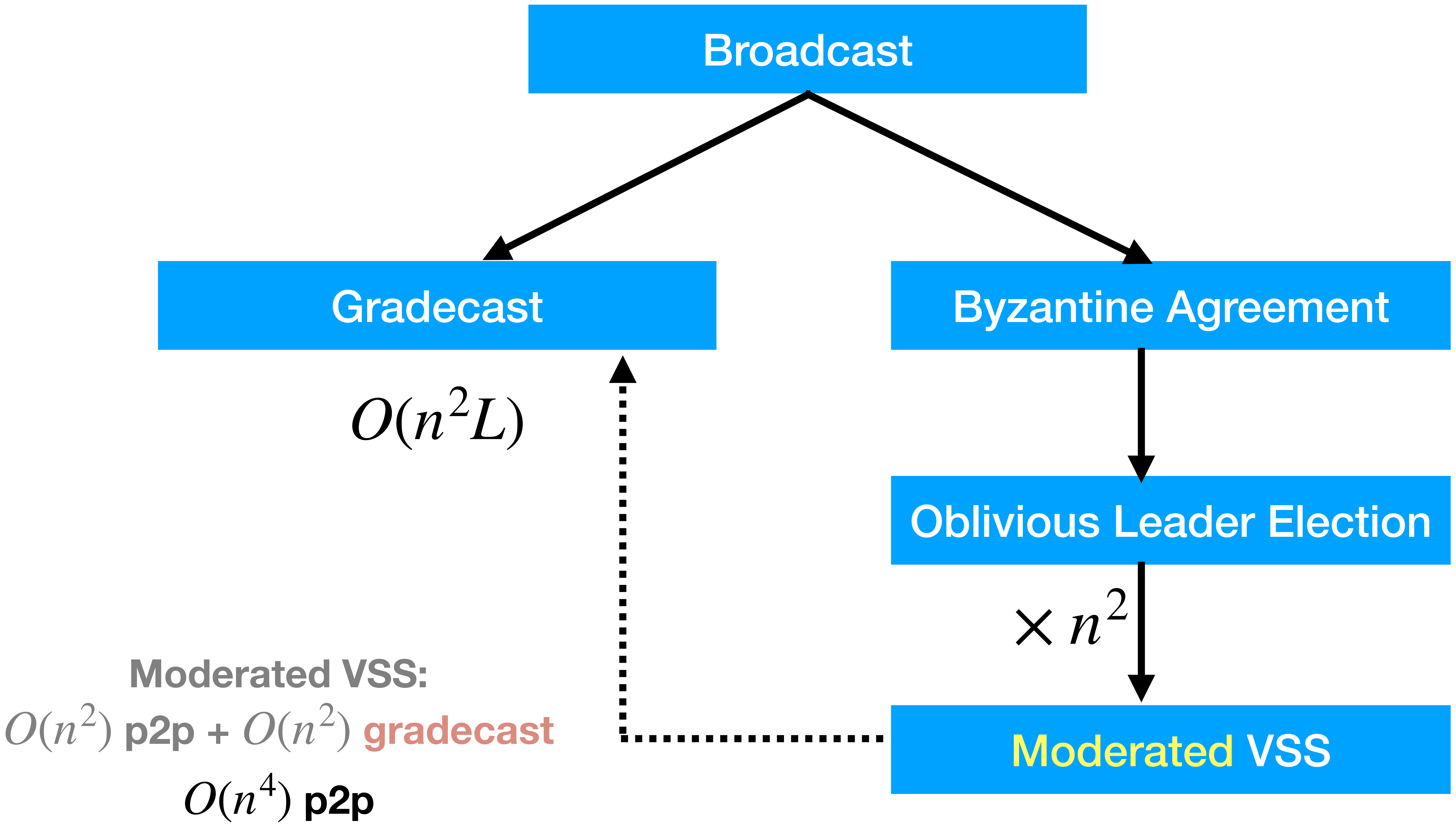
Structure of Katz and Koo



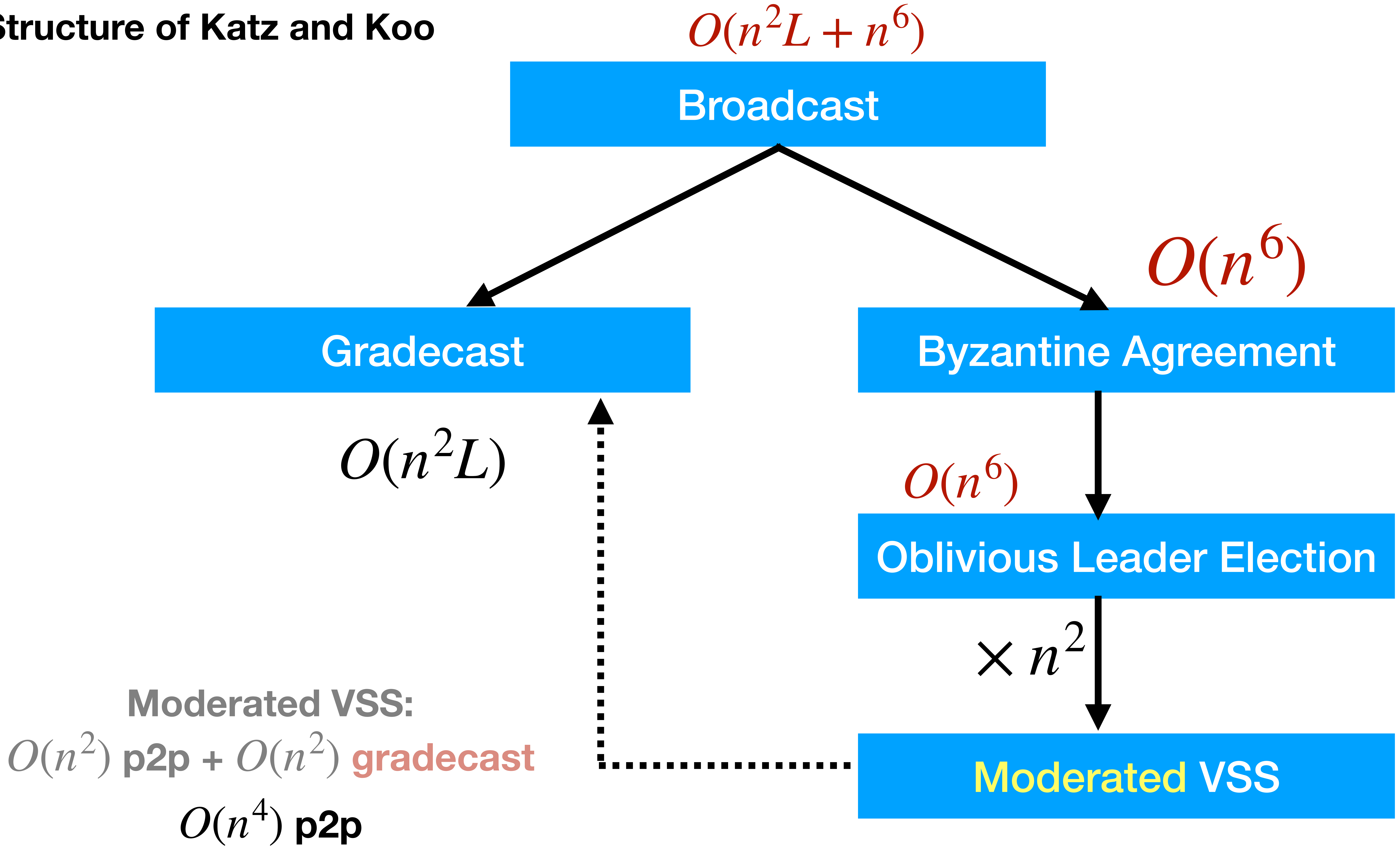
Structure of Katz and Koo



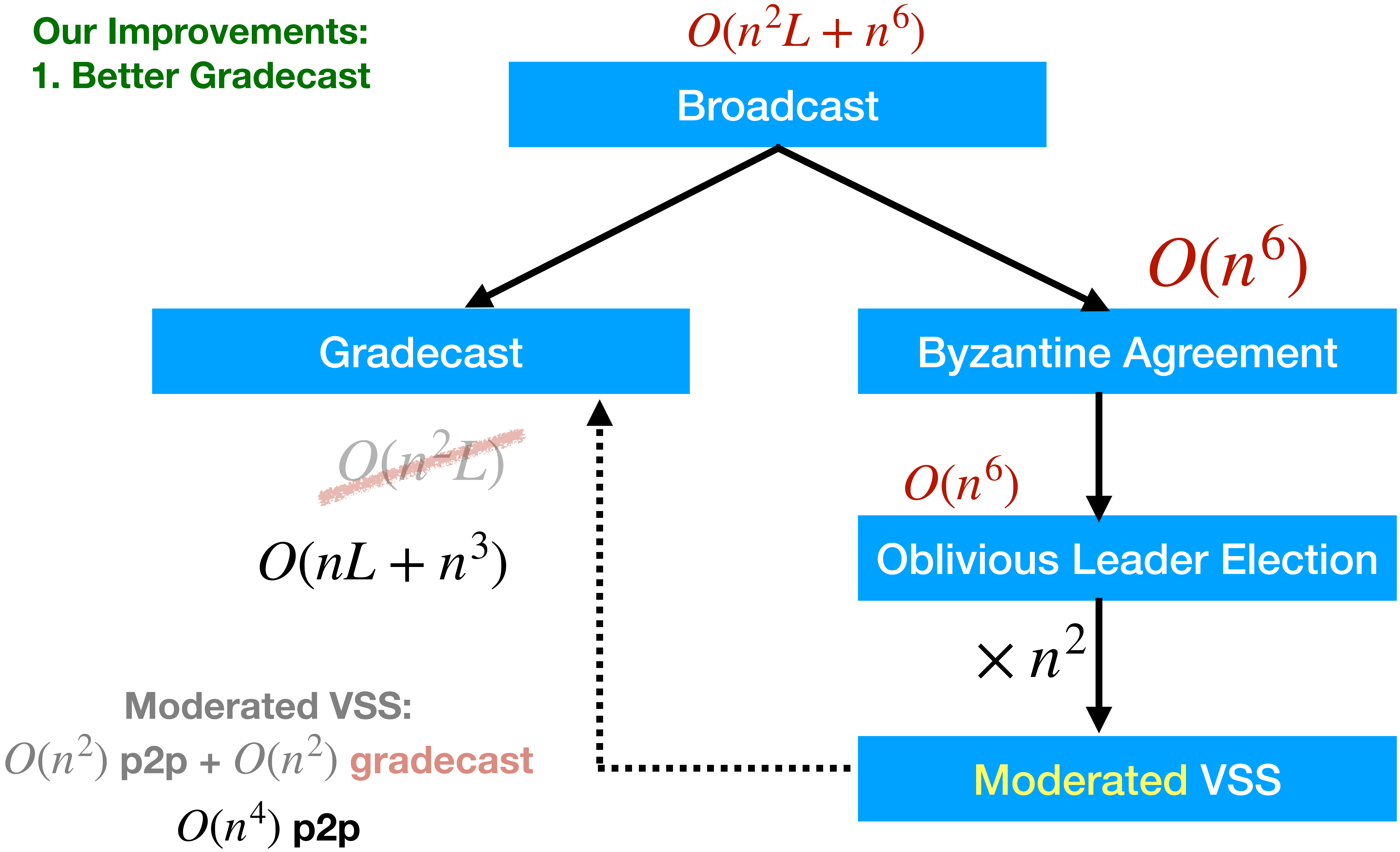
Structure of Katz and Koo

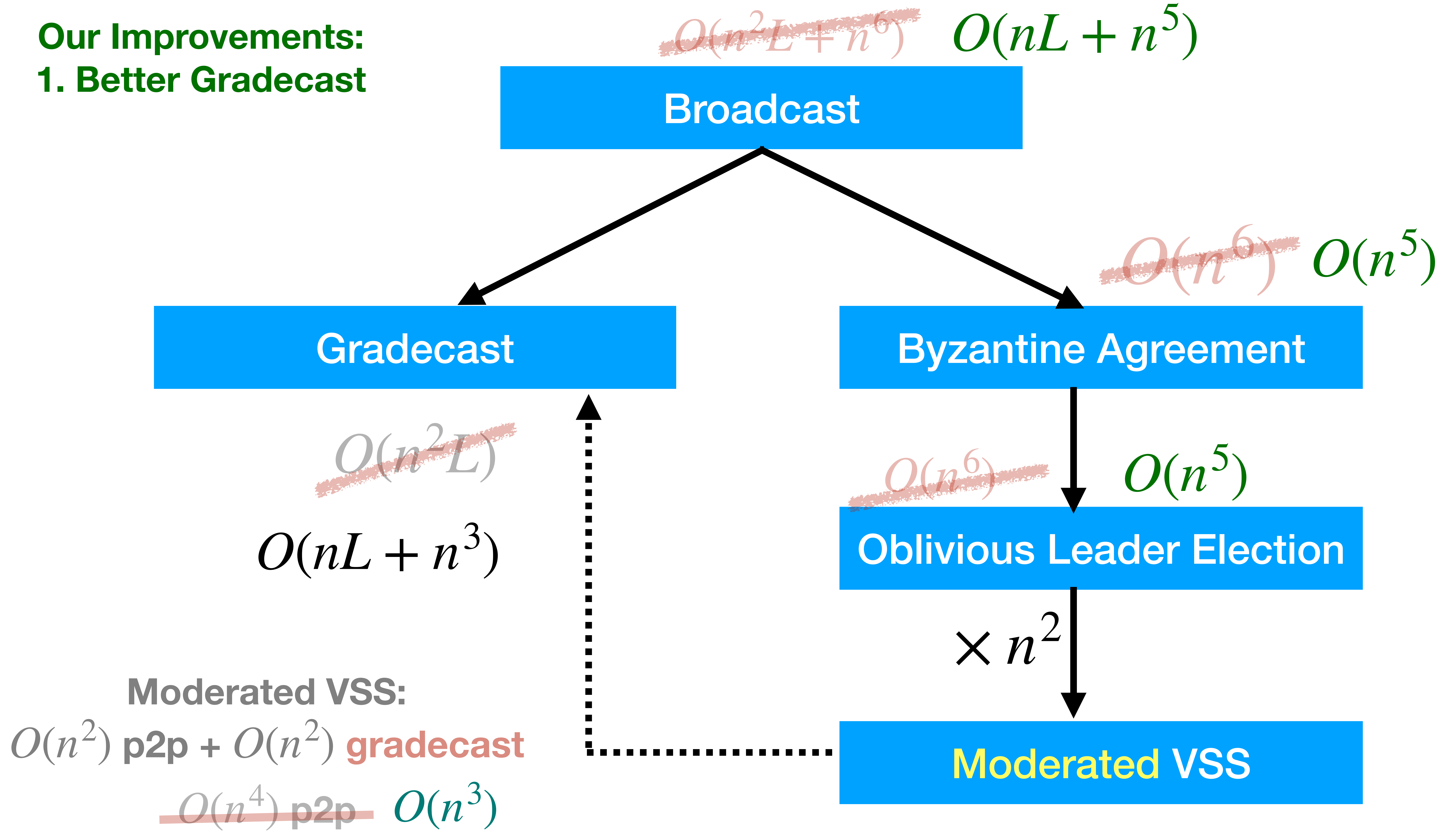


Structure of Katz and Koo

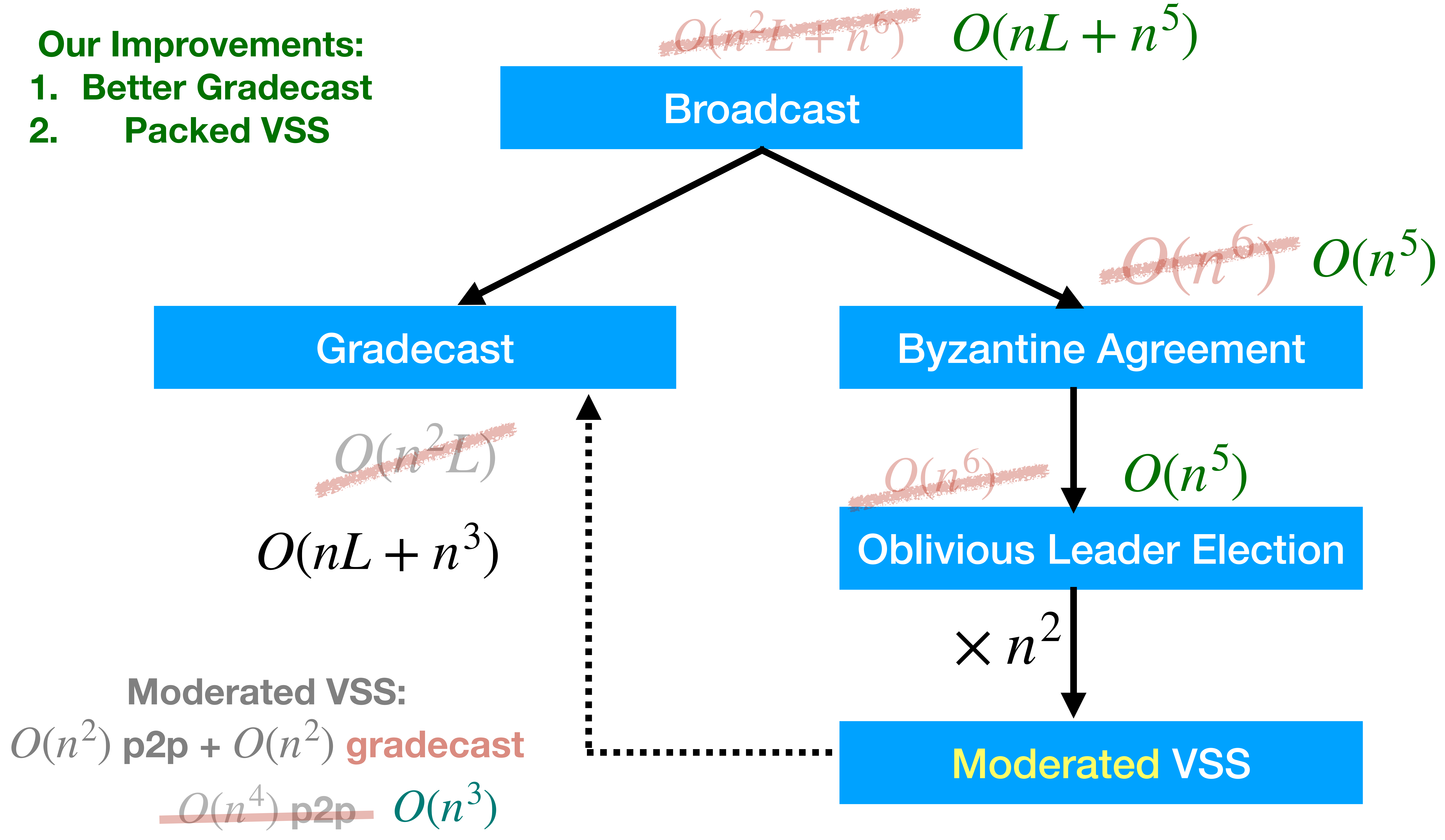


Our Improvements:
1. Better Gradecast





Our Improvements:
1. Better Gradecast
$O(n^2L + n^6)$
$O(nL + n^5)$
Broadcast
Gradecast
Byzantine Agreement
$O(n^6)$
$O(n^5)$
$O(n^2L)$
$O(nL + n^3)$
$O(n^6)$
$O(n^5)$
Oblivious Leader Election
$\times n^2$
Moderated VSS:
$O(n^2)$ p2p + $O(n^2)$ gradecast
$O(n^4)$ p2p
$O(n^3)$
Moderated VSS


Our Improvements:
1. Better Gradecast
2. Packed VSS
$O(n^2L + n^6)$
$O(nL + n^5)$
Broadcast
Gradecast
Byzantine Agreement
$O(n^6)$
$O(n^5)$
$O(n^2L)$
$O(nL + n^3)$
$O(n^6)$
$O(n^5)$
Oblivious Leader Election
$\times n^2$
Moderated VSS:
$O(n^2)$ p2p + $O(n^2)$ gradecast
$O(n^4)$ p2p
$O(n^3)$
Moderated VSS

Packed VSS

Packed VSS

- We show a novel **Verifiable Secret Sharing** protocol such that:

Packed VSS

- We show a novel **Verifiable Secret Sharing** protocol such that:
- Before: **1 secret** – $O(n^2)$ p2p + $O(n^2)$ broadcast

Packed VSS

- We show a novel **Verifiable Secret Sharing** protocol such that:
- Before: **1 secret** – $O(n^2)$ p2p + $O(n^2)$ broadcast
- Ours: $O(n)$ **secrets** – $O(n^2)$ p2p + $O(n^2)$ broadcast

Packed VSS

- We show a novel **Verifiable Secret Sharing** protocol such that:
- Before: **1 secret** – $O(n^2)$ p2p + $O(n^2)$ broadcast
- Ours: $O(n)$ **secrets** – $O(n^2)$ p2p + $O(n^2)$ broadcast

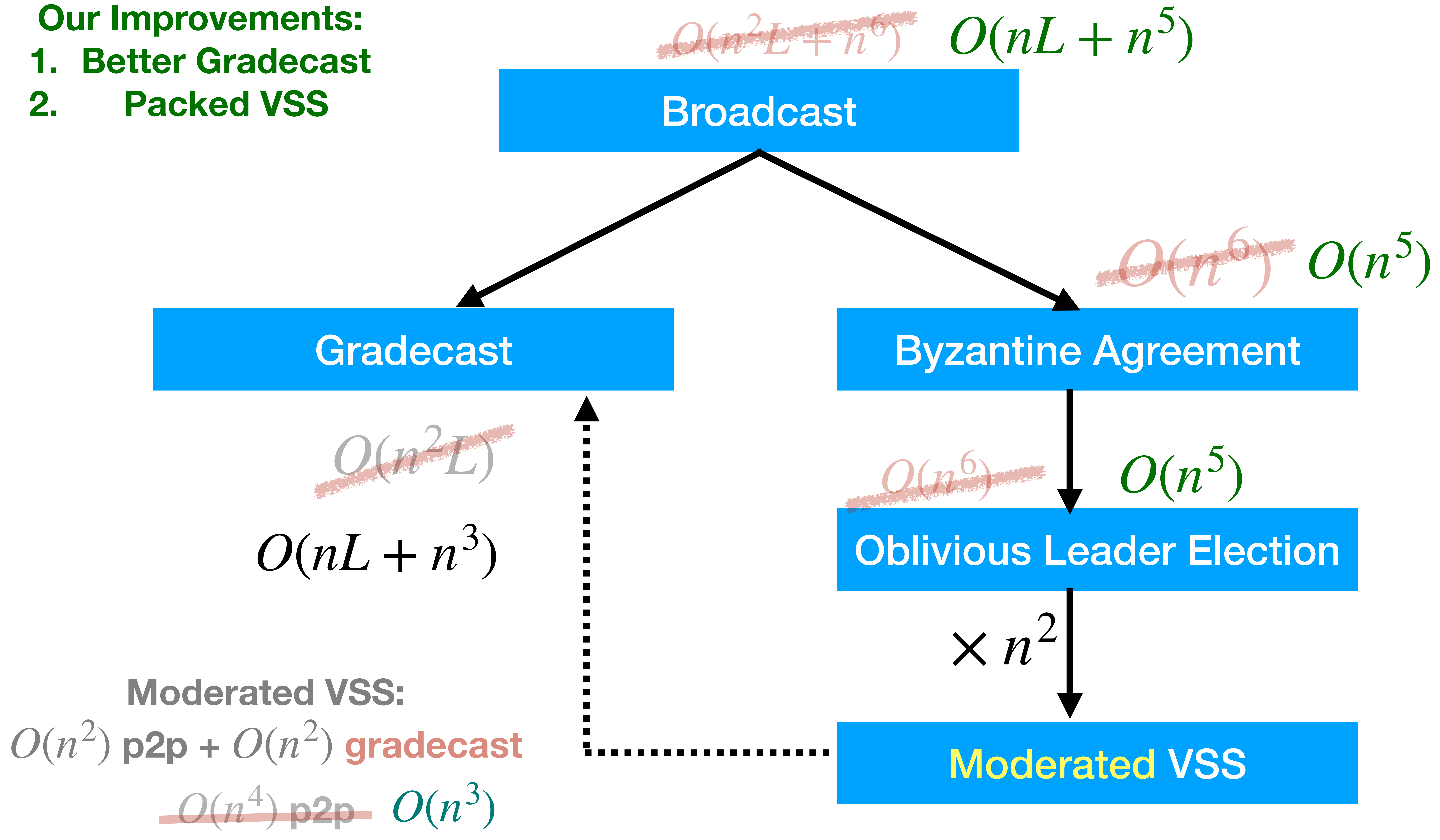
Instead of choosing a bivariate polynomial of degree at most t in x and y,
Distribute a polynomial of degree at most $2t$ in x and degree t in y

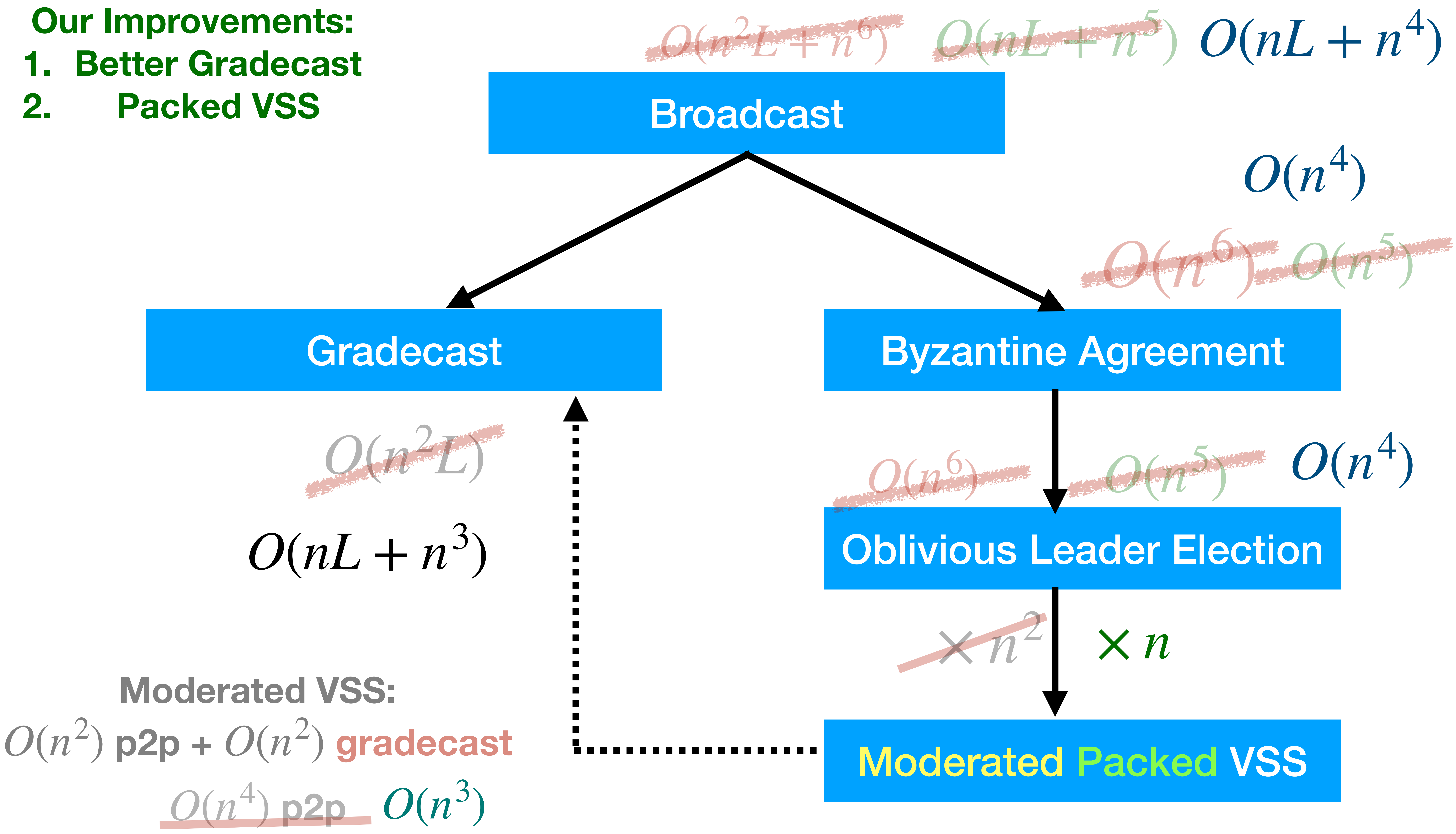
Packed VSS

- We show a novel **Verifiable Secret Sharing** protocol such that:
- Before: **1 secret** – $O(n^2)$ p2p + $O(n^2)$ broadcast
- Ours: $O(n)$ **secrets** – $O(n^2)$ p2p + $O(n^2)$ broadcast

$O(n)$ improvement over BGW!

Instead of choosing a bivariate polynomial of degree at most t in x and y,
Distribute a polynomial of degree at most $2t$ in x and degree t in y


Our Improvements:
1. Better Gradecast
2. Packed VSS
$O(n^2L + n^6)$ $O(nL + n^5)$
Broadcast
Gradecast
Byzantine Agreement
$O(n^6)$ $O(n^5)$
$O(n^2L)$
$O(nL + n^3)$
$O(n^6)$ $O(n^5)$
Oblivious Leader Election
$\times n^2$
Moderated VSS:
$O(n^2)$ p2p + $O(n^2)$ gradecast
$O(n^4)$ p2p $O(n^3)$
Moderated VSS



Our Improvements:
1. Better Gradecast
2. Packed VSS
O(n^2 L + n^6)
O(nL + n^5)
O(nL + n^4)
Broadcast
O(n^4)
O(n^6)
O(n^5)
Gradecast
Byzantine Agreement
O(n^2 L)
O(n^6)
O(n^5)
O(n^4)
O(nL + n^3)
Oblivious Leader Election
× n^2
× n
Moderated VSS:
O(n^2) p2p + O(n^2) gradecast
O(n^4) p2p
O(n^3)
Moderated Packed VSS

Conclusions

Conclusions

- $n \times$ BC(n^2) is essentially free!
  - Common communication pattern in MPC protocols
- $1 \times$ BC(L): $O(nL + n^4)$ p2p + expected $O(1)$ rounds
- Packed VSS: $O(n)$ secrets at the cost of 1

Conclusions

- $n \times \text{BC}(n^2)$ is essentially free!
    - Common communication pattern in MPC protocols
- $1 \times \text{BC(L)}$: $O(nL + n^4)$ p2p + expected $O(1)$ rounds
- Packed VSS: $O(n)$ secrets at the cost of 1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 891234

Thank You!