Round-Optimal Byzantine Agreement

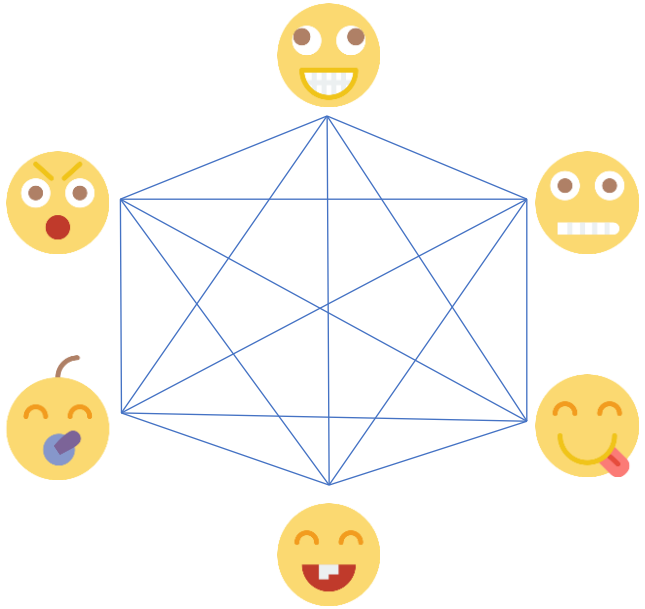
Diana Ghinea
ETH Zurich

Vipul Goyal
Carnegie Mellon University
NTT Research

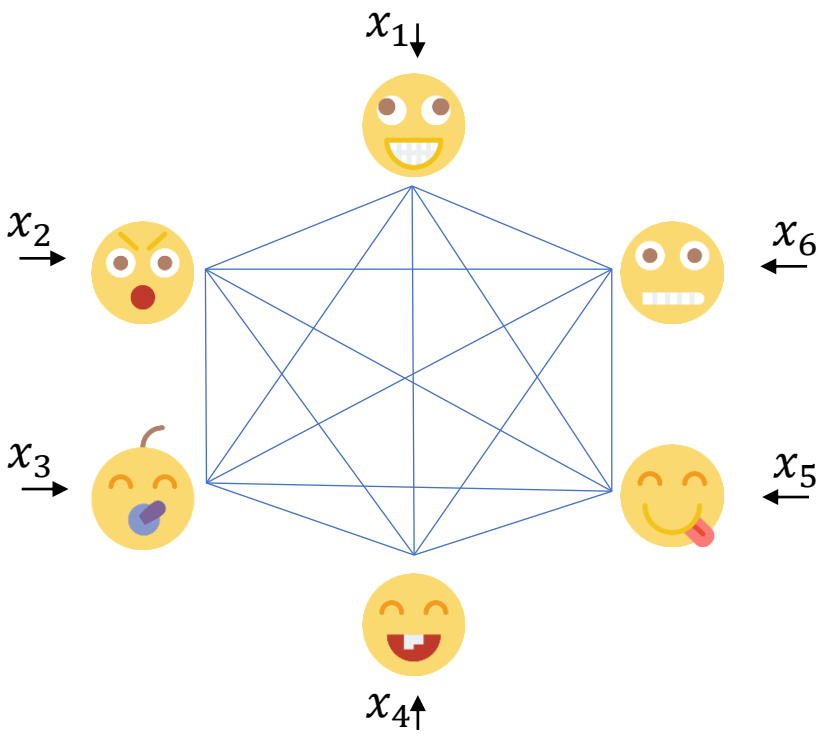
Chen-Da Liu Zhang
Carnegie Mellon University

Eurocrypt 2022

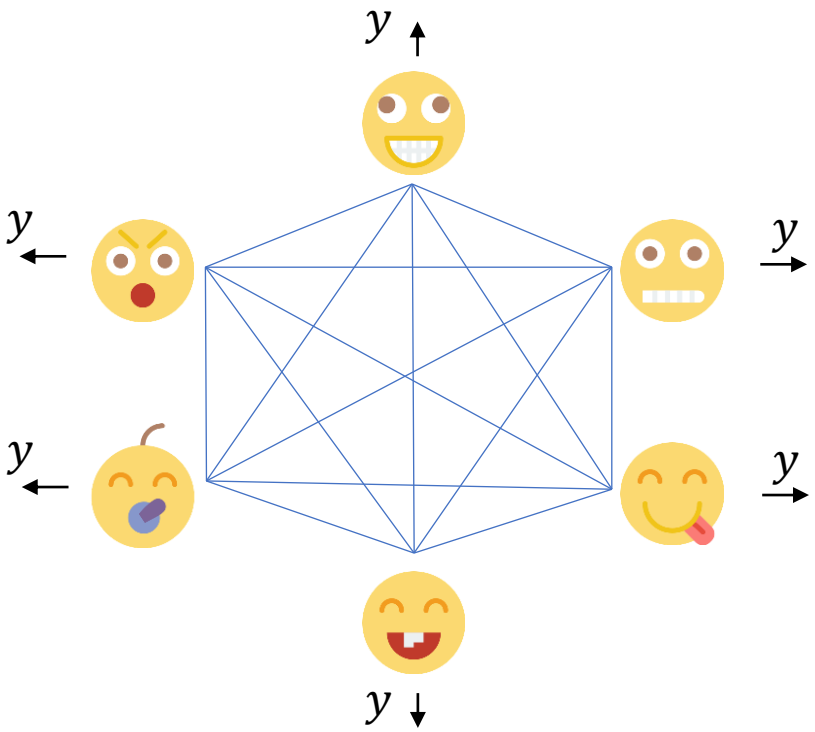
Byzantine Agreement



Byzantine Agreement

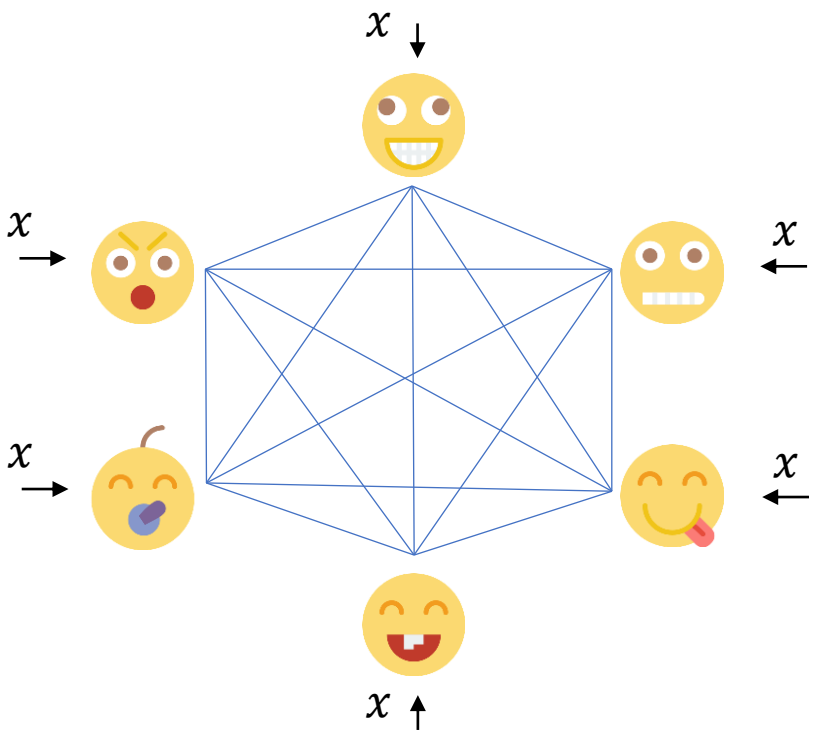


Byzantine Agreement



Consistency: All honest parties output the same value

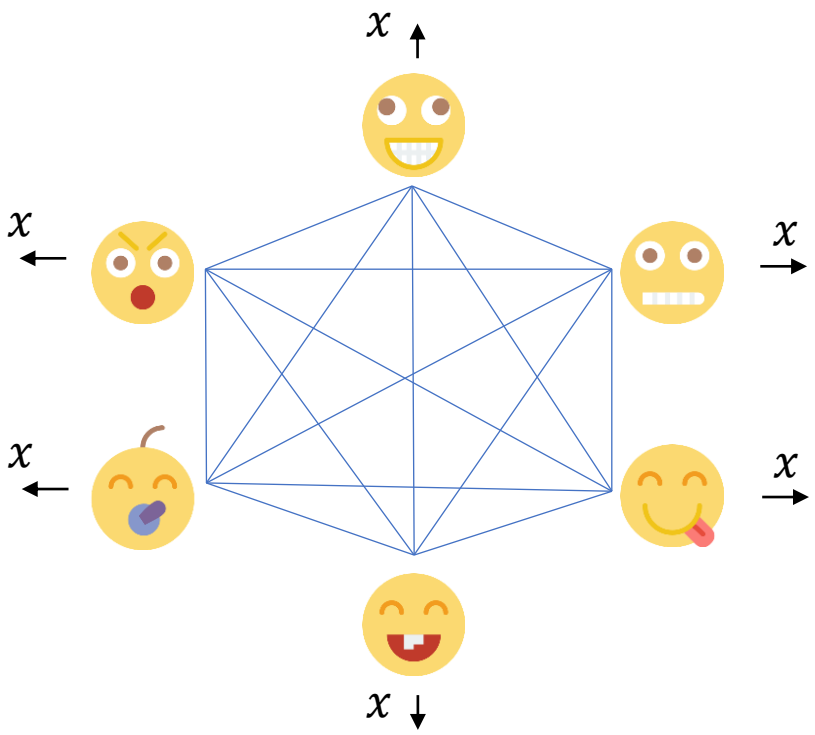
Byzantine Agreement



Consistency: All honest parties output the same value

Validity: All honest parties input the same value, they keep the same value as output

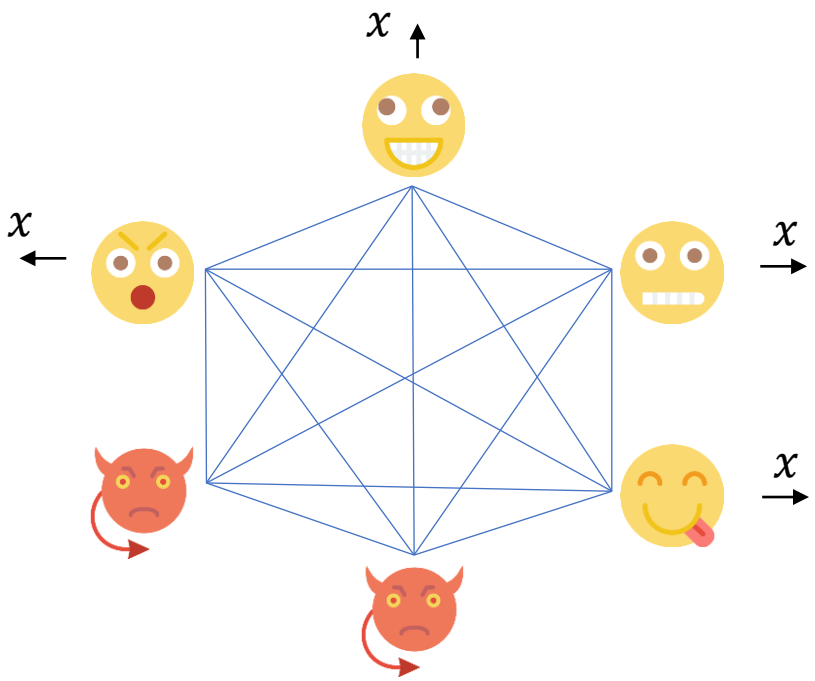
Byzantine Agreement



Consistency: All honest parties output the same value

Validity: All honest parties input the same value, they keep the same value as output

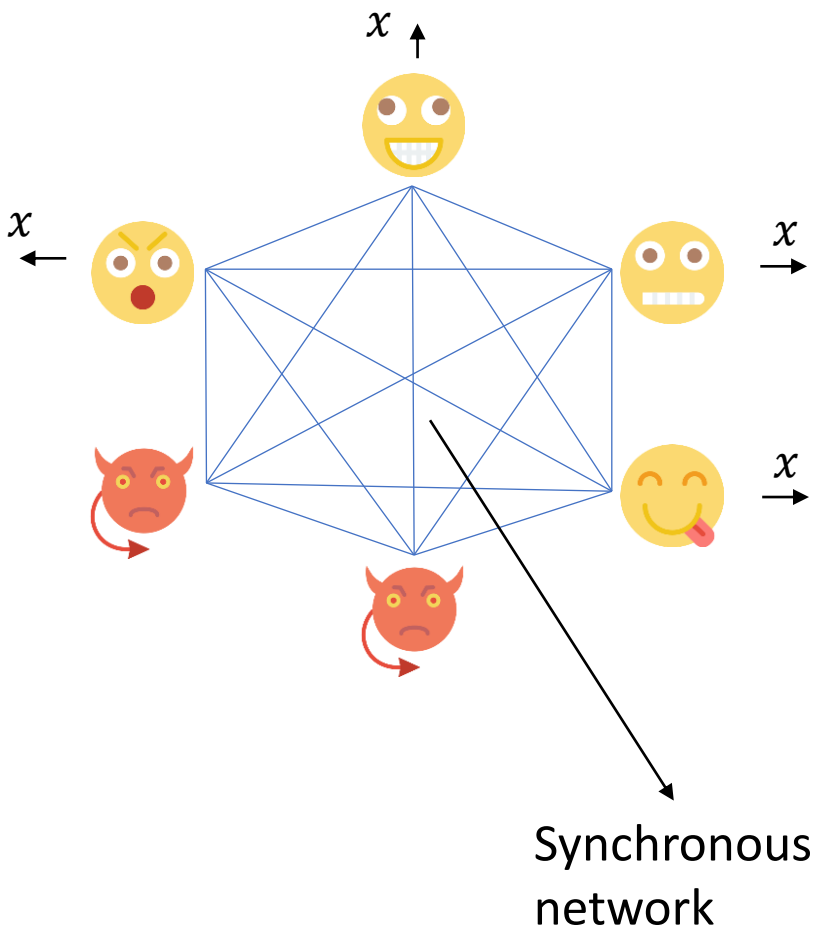
Byzantine Agreement



Consistency: All honest parties output the same value

Validity: All honest parties input the same value, they keep the same value as output

Byzantine Agreement



Consistency: All honest parties output the same value

Validity: All honest parties input the same value, they keep the same value as output

Round Efficiency

Round Efficiency

	Deterministic	
Sufficient	$t + 1$ rounds [PSL80,DS83, BGP89,CW93…]	
Necessary	$t + 1$ rounds [DS83]	

Round Efficiency

	Deterministic	Randomized
Sufficient	$t+1$ rounds [PSL80,DS83, BGP89,CW93…]	cr rounds with $\leq 2^{-r}$ error [FM97,FG03,KK06, Mic16,MV17, FLL21…]
Necessary	$t+1$ rounds [DS83]	$t=\theta(n)$: r rounds incurs $\geq (cr)^{-r}$ error [KY84]

Round Efficiency

	Deterministic	Randomized
Sufficient	$t+1$ rounds [PSL80,DS83, BGP89,CW93…]	cr rounds with $\leq 2^{-r}$ error [FM97,FG03,KK06, Mic16,MV17, FLL21…] $t=(1-\epsilon)\frac{n}{2}$: $3r$ rounds with $\leq (cr)^{-r}$ error [GGL22]
Necessary	$t+1$ rounds [DS83]	$t=\theta(n)$: r rounds incurs $\geq (cr)^{-r}$ error [KY84]

Seminal Paradigm [Rabin,Feldman-Micali]

Weak Consensus

Input $x_i \in \{0,1\}$; Output $y_i \in \{0, \perp, 1\}$

Weak Consensus

Input $x_i \in \{0,1\}$; Output $y_i \in \{0, \perp, 1\}$

0	$\perp$	1

Weak Consensus

Input $x_i \in \{0,1\}$; Output $y_i \in \{0, \perp, 1\}$

0	$\perp$	1

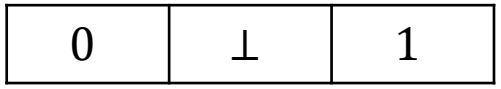
Validity

If $\forall$ honest P_i inputs $x_i = x$, then $y_i = x$

$x = 0$:	**0**	$\perp$	1
$x = 1$:	0	$\perp$	**1**

Weak Consensus

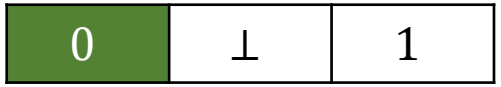
Input $x_i \in \{0,1\}$; Output $y_i \in \{0, \perp, 1\}$



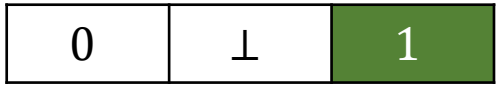
Validity

If ∀ honest P_i inputs $x_i = x$, then $y_i = x$

$x = 0$:

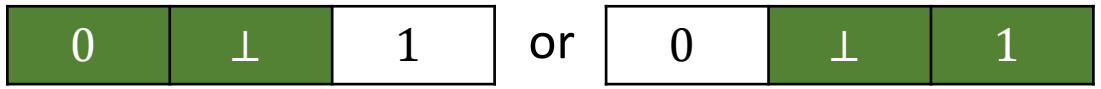


$x = 1$:



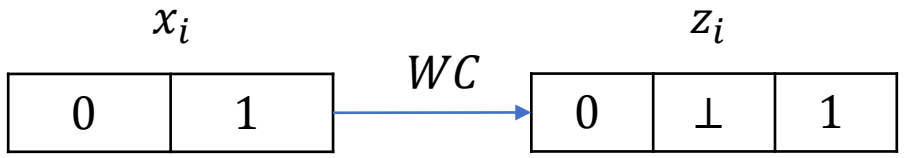
Weak Consistency

$\exists b \in \{0,1\}$ s.t. all honest P_i output $y_i \in \{b, \perp\}$



Seminal Paradigm

For $k = 1 \ldots r$



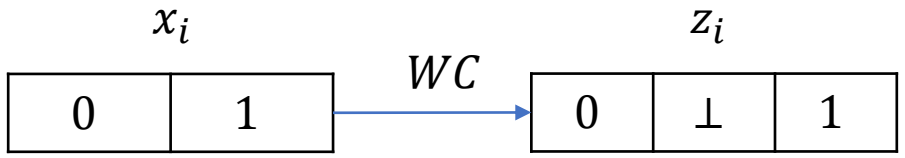
Each P_i gets a common random $c \leftarrow_{\$} \{0,1\}$

P_i sets $y_i = z_i$ if $z_i \in \{0,1\}$
sets $y_i = c$ if $z_i \in \perp$

Set $x_i = y_i$

Seminal Paradigm

For $k = 1 \ldots r$



Each P_i gets a common random $c \leftarrow_{\$} \{0,1\}$

P_i sets $y_i = z_i$ if $z_i \in \{0,1\}$
sets $y_i = c$ if $z_i \in \perp$

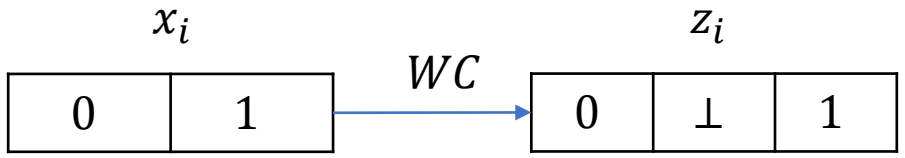
Set $x_i = y_i$

Validity

If $\forall$ honest P_i inputs $x_i = x$, then $z_i = x$
$\Rightarrow y_i = x$ (no party ever adopts the coin)

Seminal Paradigm

For $k = 1 \ldots r$



Each P_i gets a common random $c \leftarrow_{\$} \{0,1\}$

P_i sets $y_i = z_i$ if $z_i \in \{0,1\}$
sets $y_i = c$ if $z_i \in \perp$

Set $x_i = y_i$

Validity

If ∀ honest P_i inputs $x_i = x$, then $z_i = x$
$\Rightarrow y_i = x$ (no party ever adopts the coin)

Consistency

In an iteration:

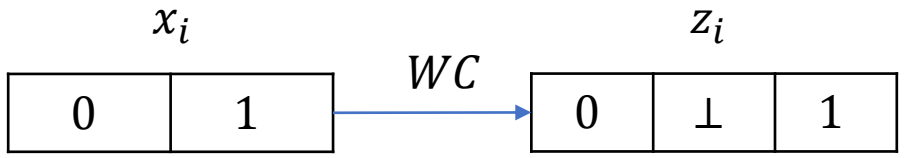
All parties output c

If $c = 0$, all parties output 0

$\Pr[agree] \geq \frac{1}{2}$

Seminal Paradigm

For $k = 1 \ldots r$



Each P_i gets a common random $c \leftarrow_{\$} \{0,1\}$

P_i sets $y_i = z_i$ if $z_i \in \{0,1\}$
sets $y_i = c$ if $z_i \in \perp$

Set $x_i = y_i$

Each iteration takes ≥ 2 rounds
$\Rightarrow$ **$2r$ rounds for agreement with probability $1 - 2^{-r}$**

Validity

If $\forall$ honest P_i inputs $x_i = x$, then $z_i = x$
$\Rightarrow y_i = x$ (no party ever adopts the coin)

Consistency

In an iteration:

All parties output c

If $c = 0$, all parties output 0

$\Pr[agree] \geq \frac{1}{2}$

Expand-and-Extract [FLL21,GGL22]

Proxcensus with s slots

Input $x_i \in \{0,1\}$; Output a slot $y_i \in \{1, \dots, s\}$

Proxcensus with s slots

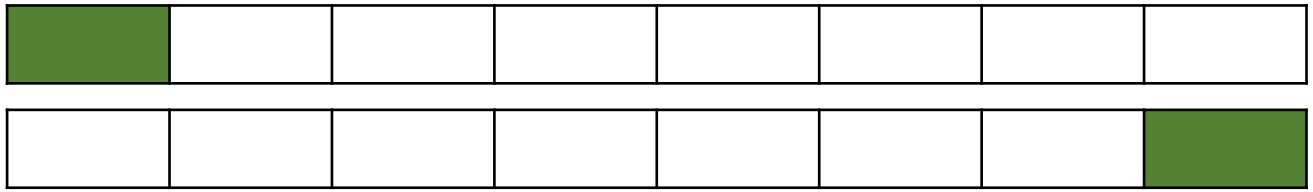
Input $x_i \in \{0,1\}$; Output a slot $y_i \in \{1, \dots, s\}$

Validity

If $\forall$ honest P_i inputs 0 (resp. 1), then y_i is the left- (right-) most slot

$x = 0$:

$x = 1$:



Proxcensus with s slots

Input $x_i \in \{0,1\}$; Output a slot $y_i \in \{1, \dots, s\}$

Validity

If $\forall$ honest P_i inputs 0 (resp. 1), then y_i is the left- (right-) most slot

$x = 0$:

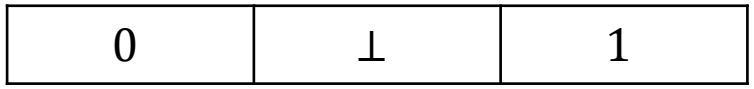
$x = 1$:

Consistency

Honest parties' outputs lie within two consecutive slots

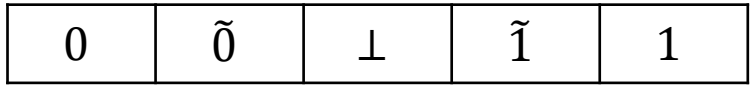
Proxcensus with s slots

Examples



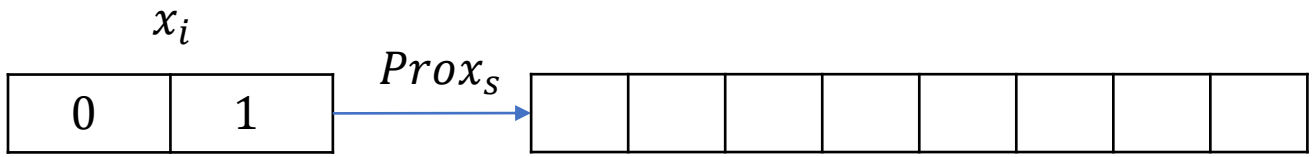
$Prox_3$ is Weak Consensus / Crusader's agreement

$Prox_4$ is {0,1}-Graded Consensus

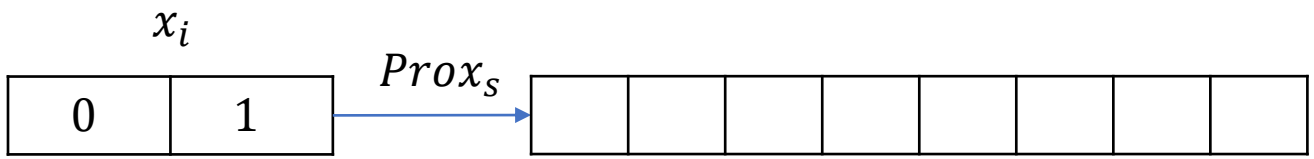


$Prox_5$ is {0,1,2}-Graded Consensus

Expand-and-Extract

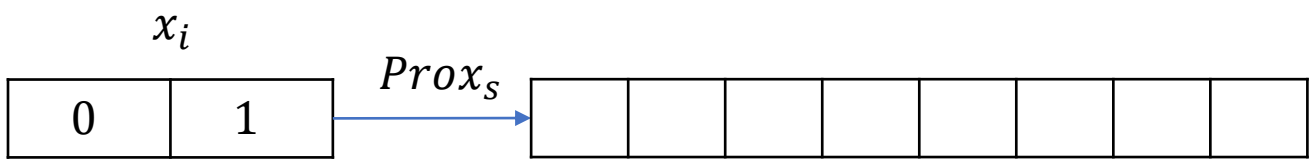


Expand-and-Extract

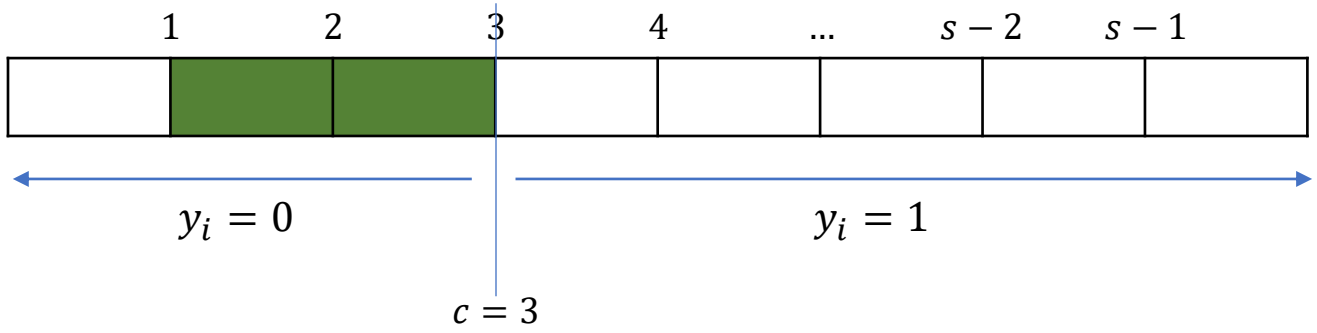


Each P_i gets a common random $c \leftarrow_{\$} \{1, s-1\}$

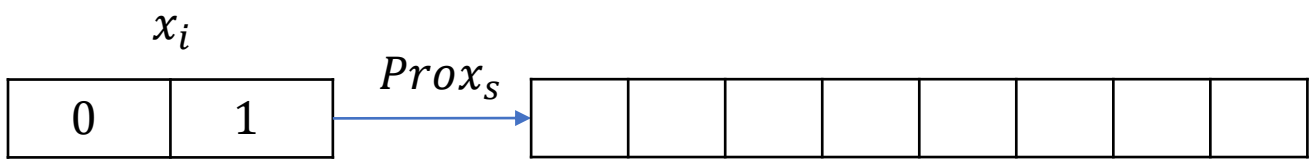
Expand-and-Extract



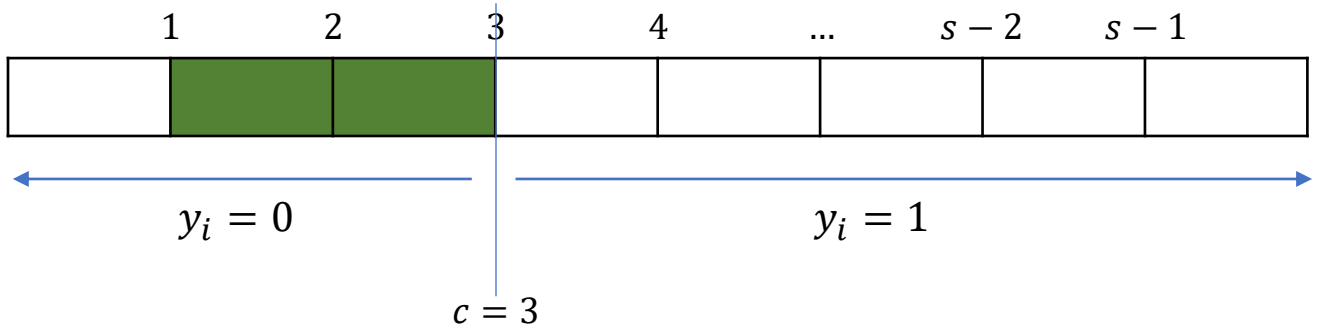
Each P_i gets a common random $c \leftarrow_{\$} \{1, s-1\}$



Expand-and-Extract



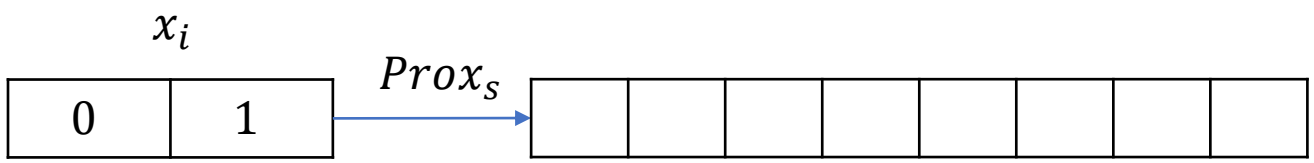
Each P_i gets a common random $c \leftarrow_{\$} \{1, s-1\}$



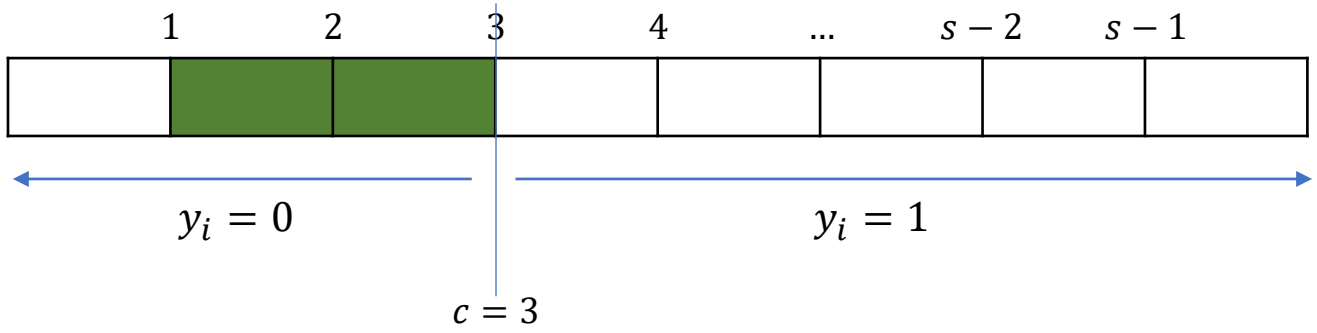
Validity

If ∀ honest P_i inputs $x_i = x \in \{0,1\}$, then no matter the coin value, it holds that $y_i = x$

Expand-and-Extract



Each P_i gets a common random $c \leftarrow_{\$} \{1, s-1\}$



Validity

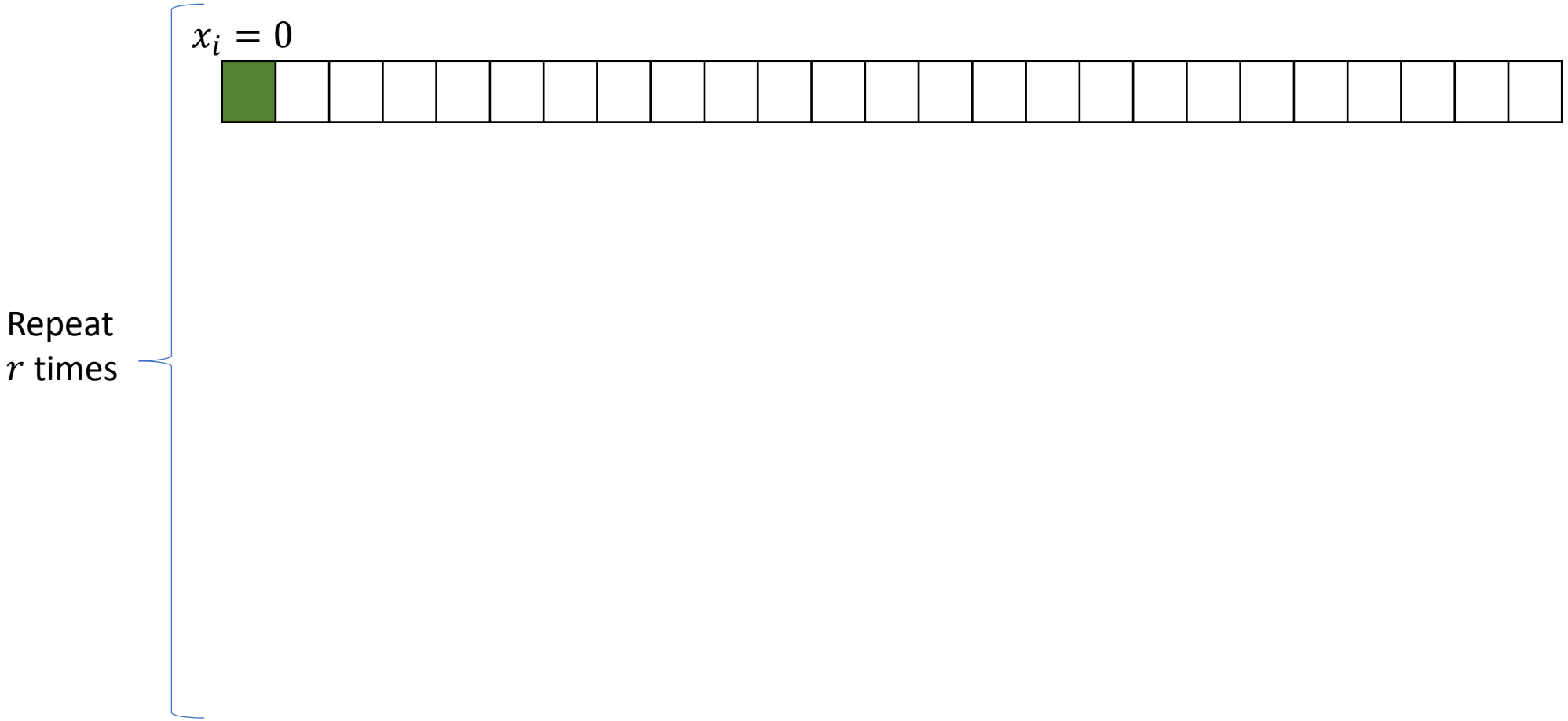
If ∀ honest P_i inputs $x_i = x \in \{0,1\}$,
then no matter the coin value,
it holds that $y_i = x$

Consistency

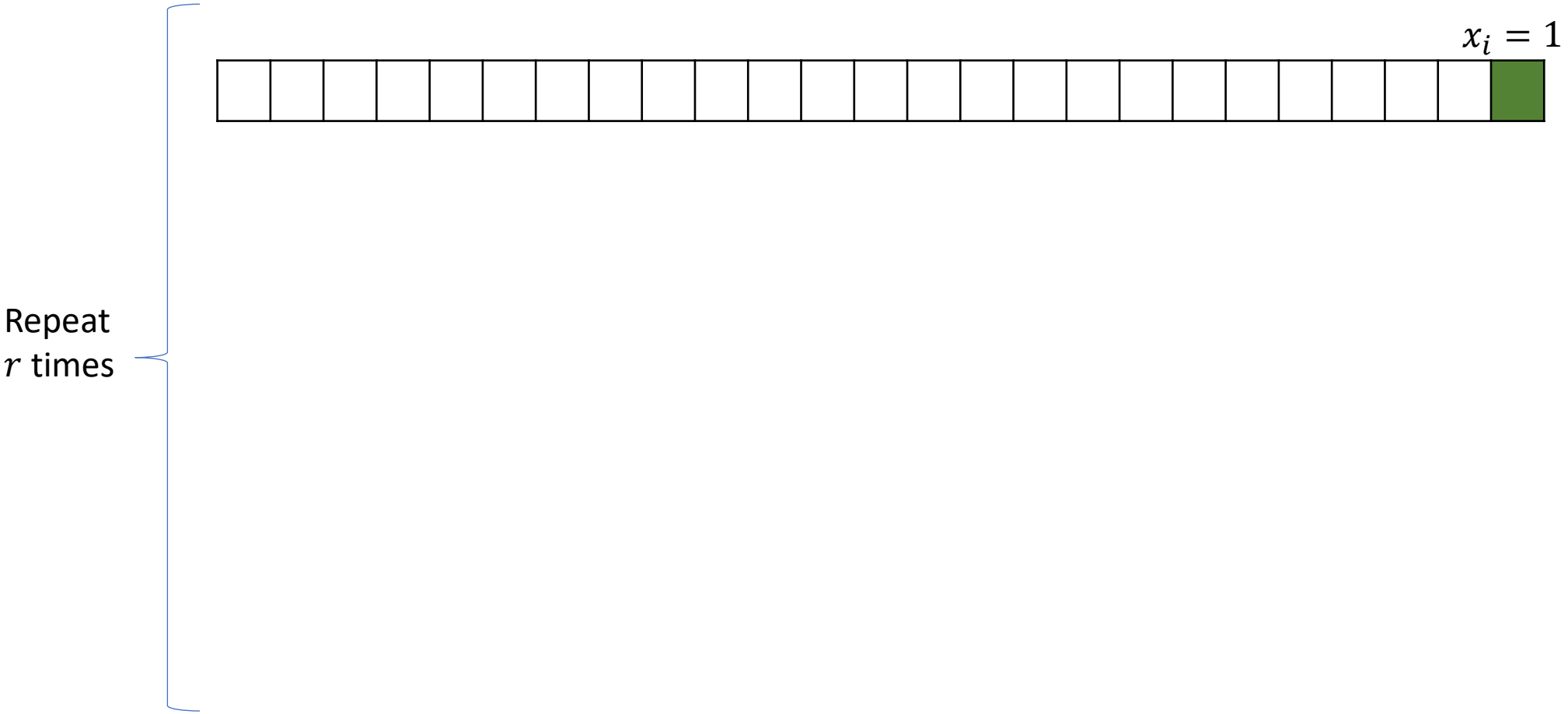
Only one coin value causes disagreement

$\Pr[agree] \geq 1 - \frac{1}{s-1}$

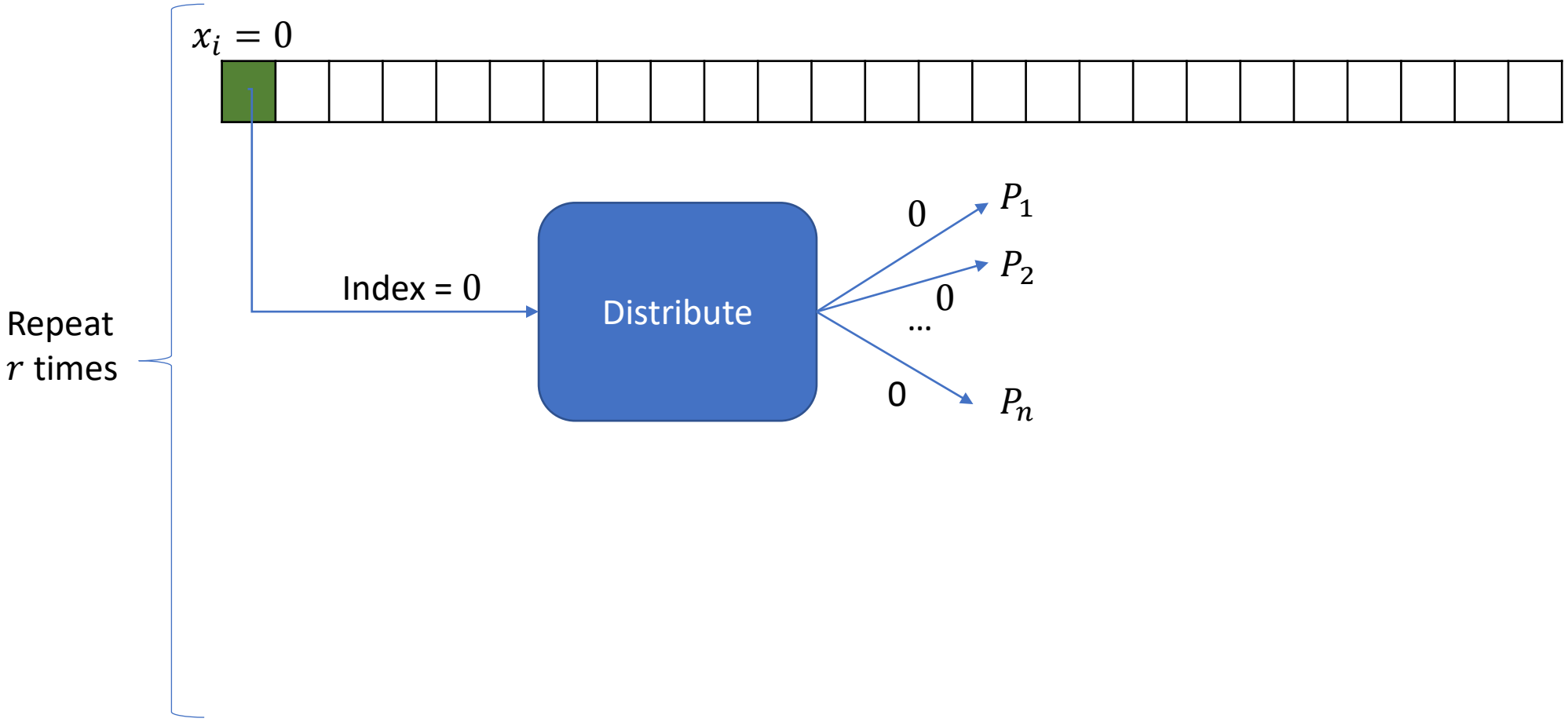
Expansion with $\sim \mathbf{r}^{\mathbf{r}}$ slots in $\mathbf{3r}$ rounds



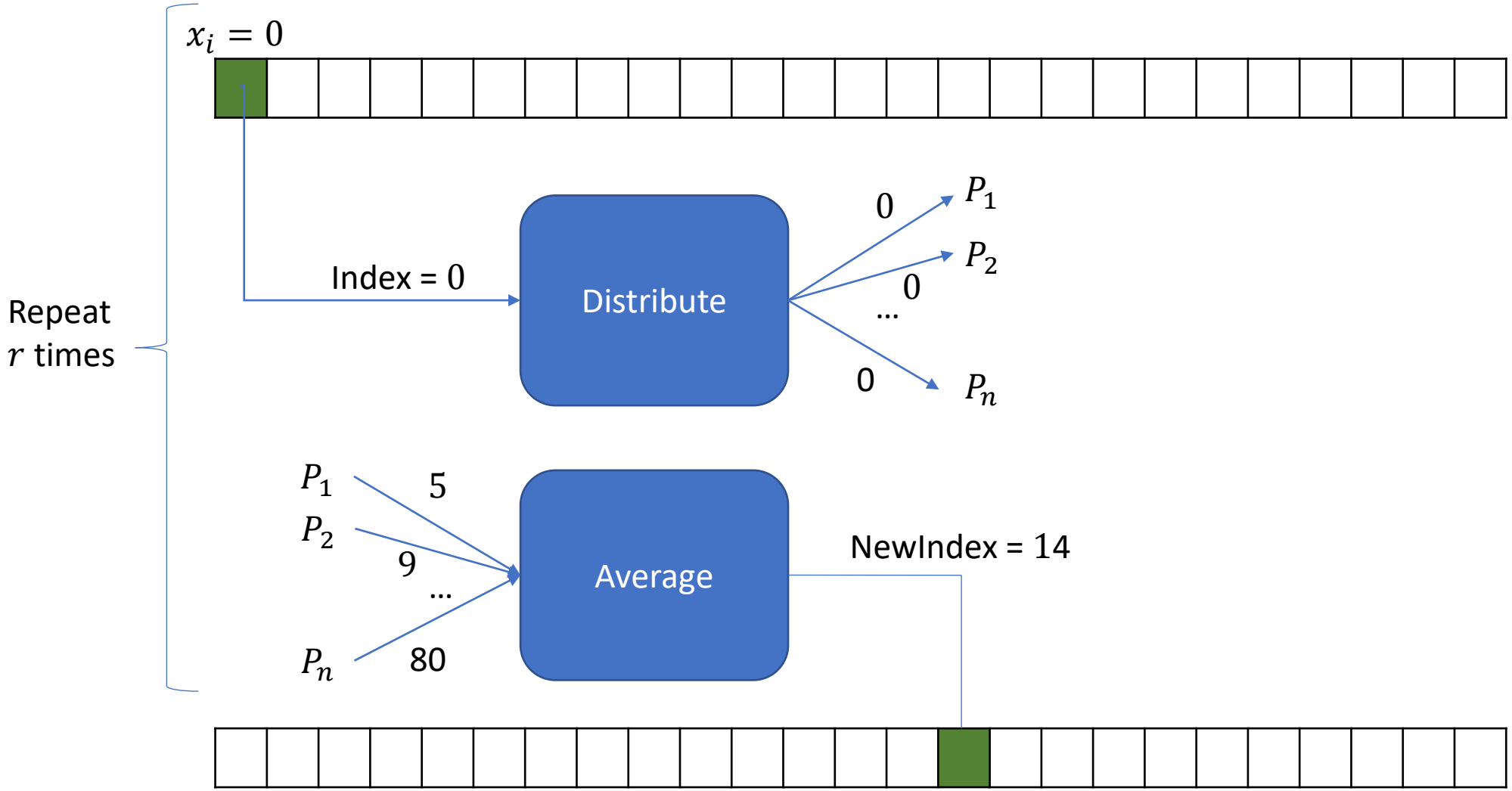
Expansion with $\sim \mathbf{r}^{\mathbf{r}}$ slots in $\mathbf{3r}$ rounds



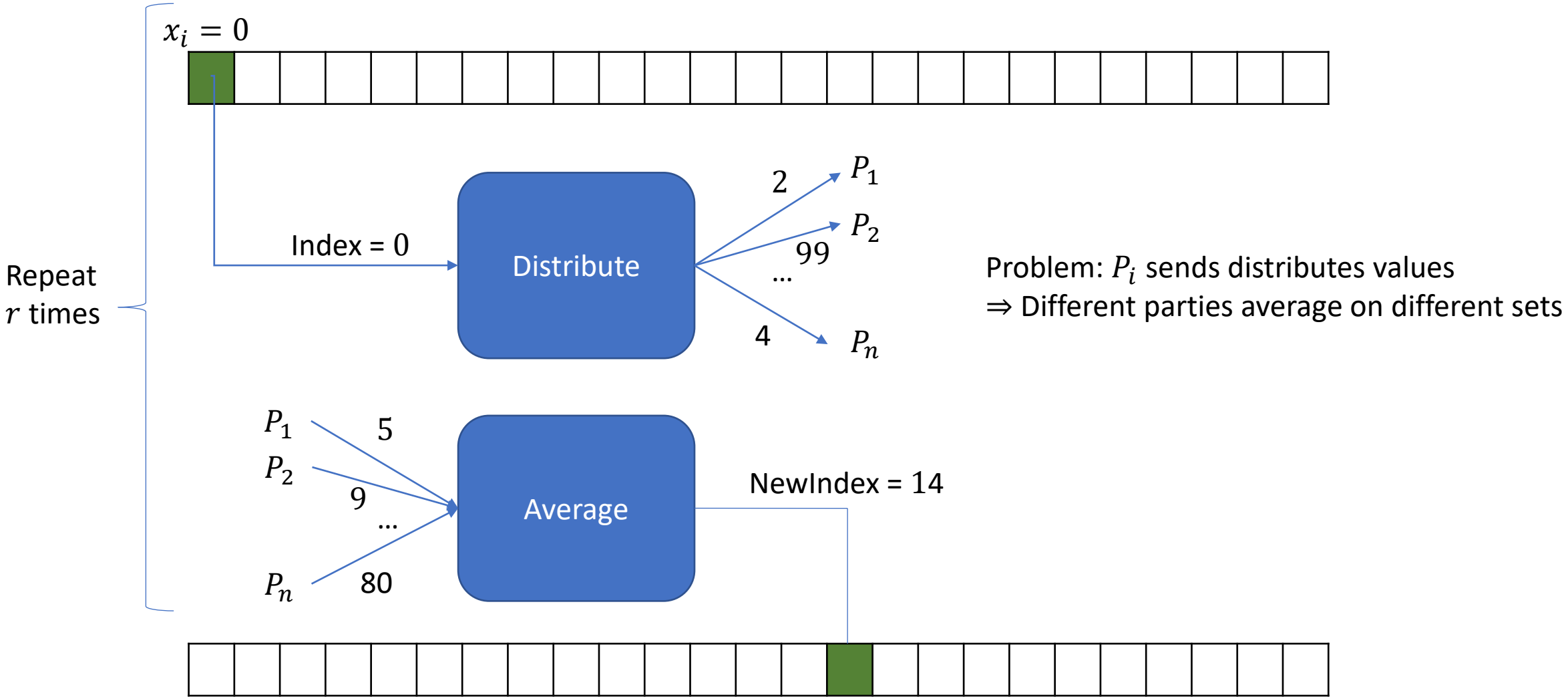
Expansion with $\sim \mathbf{r}^{\mathbf{r}}$ slots in $\mathbf{3r}$ rounds



Expansion with $\sim \mathbf{r}^{\mathbf{r}}$ slots in $\mathbf{3r}$ rounds

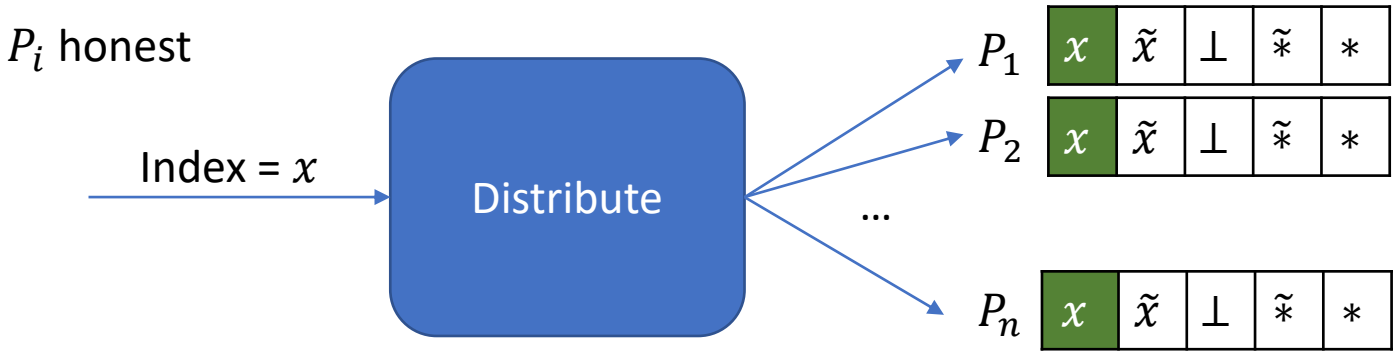


Expansion with $\sim \mathbf{r}^{\mathbf{r}}$ slots in $\mathbf{3r}$ rounds

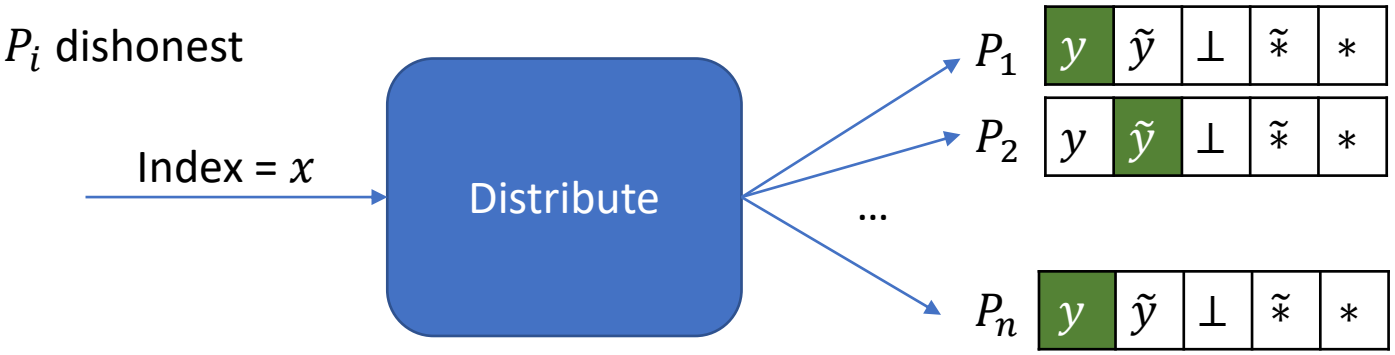


Problem: P_i sends distributes values
⇒ Different parties average on different sets

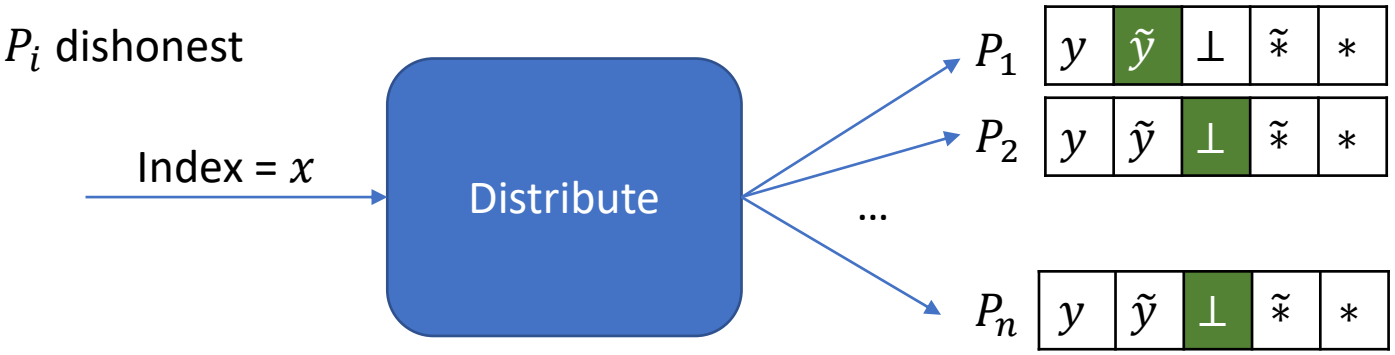
Distribute + Average



Distribute + Average



Distribute + Average

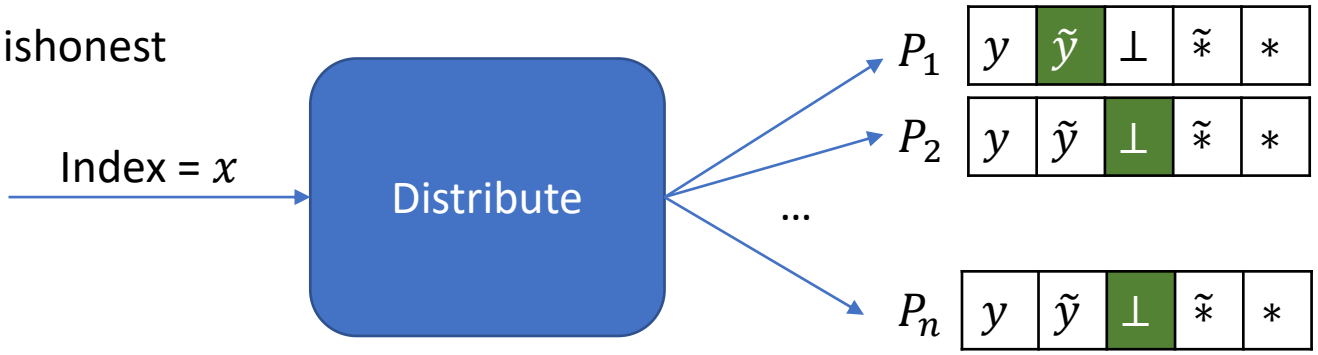


Distribute + Average

Each P_j has local set C of recognized corrupted parties

P_i dishonest

Index = x

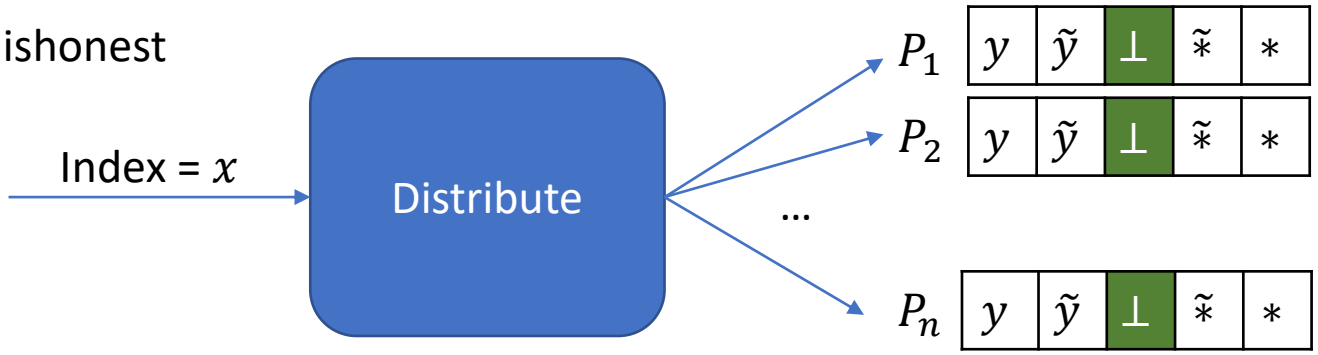


Distribute + Average

Each P_j has local set C of recognized corrupted parties

P_i dishonest

Index = x



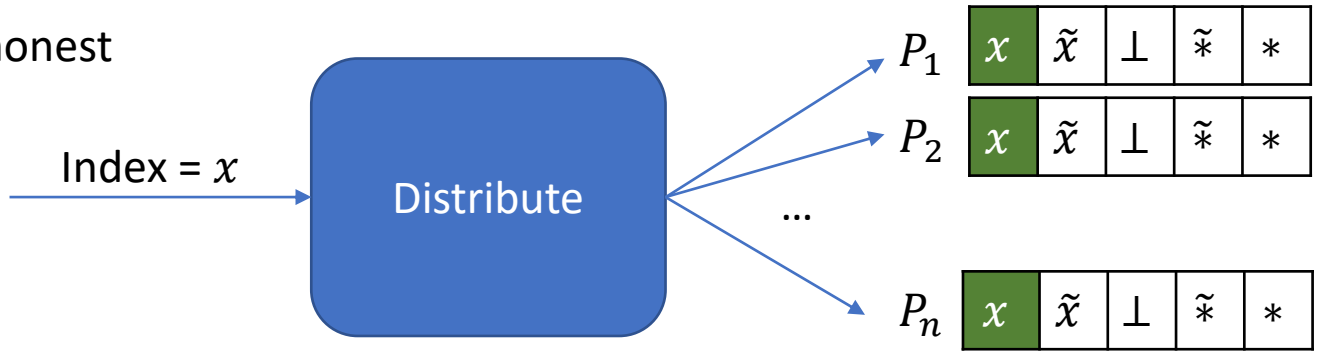
If P_i is identified by all honest parties, then the output is $\perp$

Distribute + Average

Local set C of recognized corrupted parties

P_i honest

Index = x



Discard $\perp$ values, let $C_0 = \{P_j | \, y_j = \perp\}$, $C_1 = \{P_j | \, y_j = \tilde{y}\}$

NewIndex = $Avg(M)$

M set of values after trimming $t - |C_0|$ highest and lowest values of non-$\perp$ values

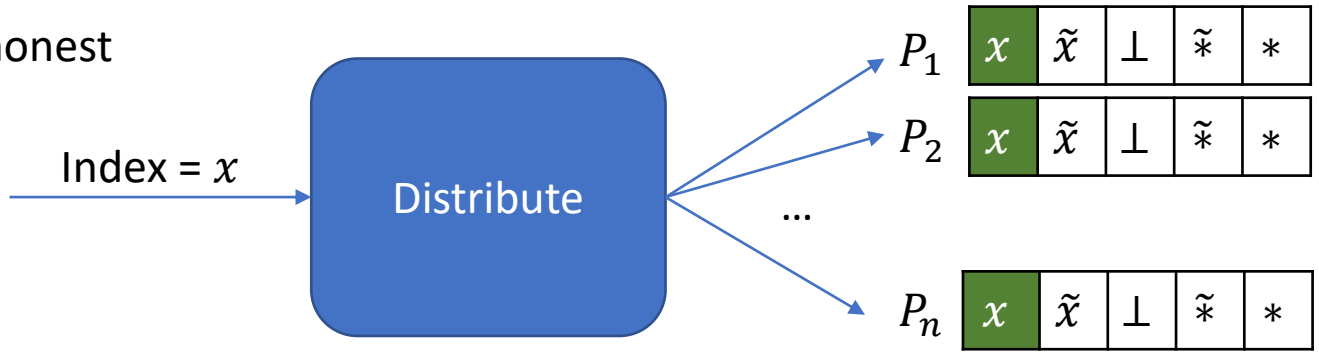
Update the corrupted set $C = C \cup C_0 \cup C_1$

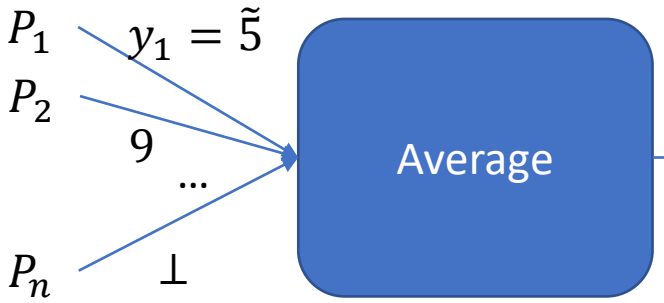
Distribute + Average

Local set C of recognized corrupted parties

P_i honest

Index = x





Discard $\perp$ values, let $C_0 = \{P_j | \, y_j = \perp\}$, $C_1 = \{P_j | \, y_j = \tilde{y}\}$

NewIndex = $Avg(M)$

M set of values after trimming $t - |C_0|$ highest and lowest values of non-$\perp$ values

Example: $|C_0| = 3, \mathrm{t} = 5$

1	3	$\tilde{3}$	4	4	$\tilde{4}$	15	21	$\widetilde{22}$	85	88	94

Update the corrupted set $C = C \cup C_0 \cup C_1$

Distribute + Average

Local set C of recognized corrupted parties

P_i honest

Index = x

Distribute

P_1	x	$\tilde{x}$	$\perp$	$\tilde{*}$	$*$
P_2	x	$\tilde{x}$	$\perp$	$\tilde{*}$	$*$
...					
P_n	x	$\tilde{x}$	$\perp$	$\tilde{*}$	$*$

P_1 $y_1 = \tilde{5}$

P_2 9

...

P_n $\perp$

Average

Discard $\perp$ values, let $C_0 = \{P_j | \, y_j = \perp\}$, $C_1 = \{P_j | \, y_j = \tilde{y}\}$

NewIndex = $Avg(M)$

M set of values after trimming $t - |C_0|$ highest and lowest values of non-$\perp$ values

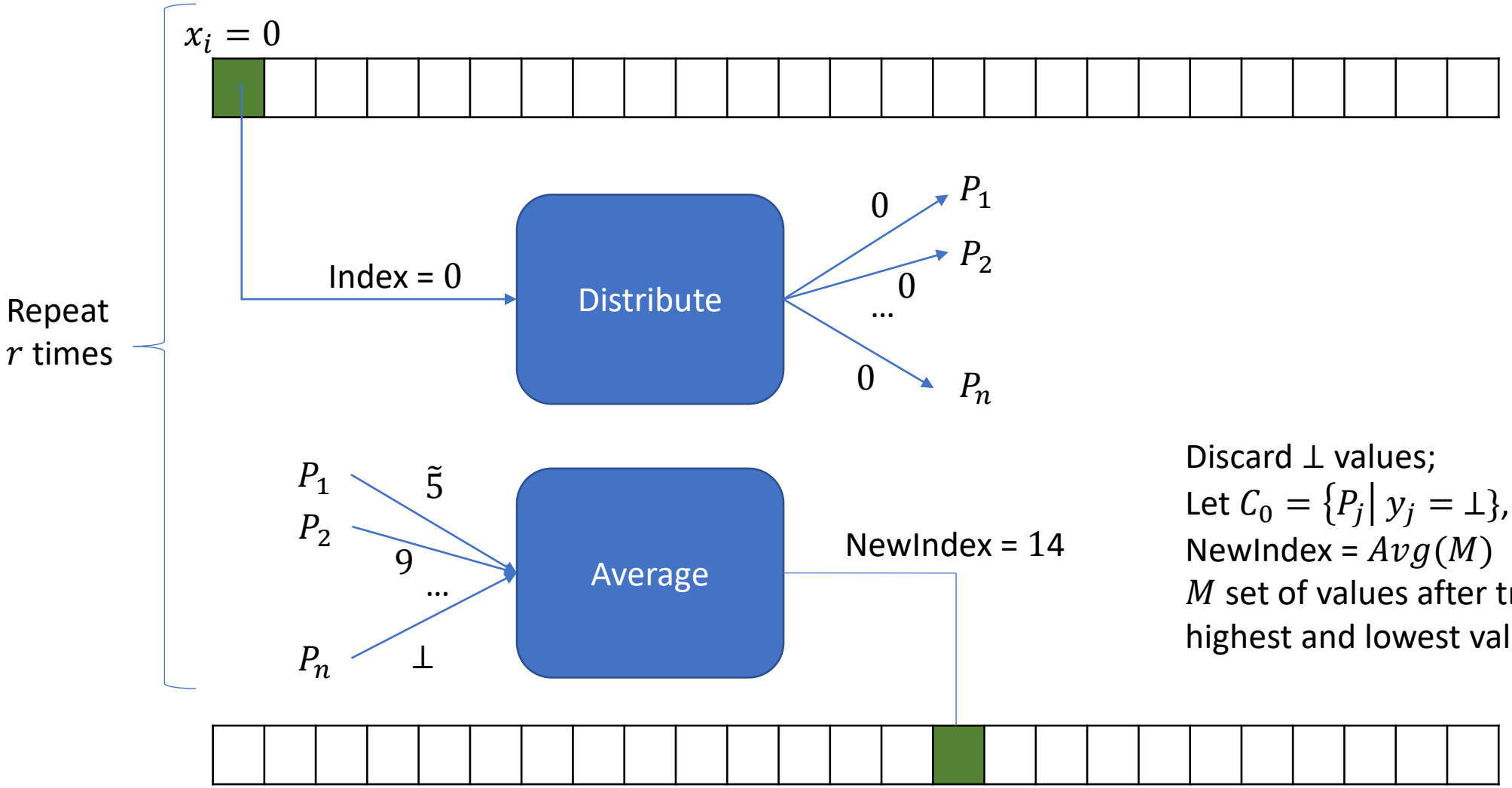
Example: $|C_0| = 3, t = 5$

1	3	$\tilde{3}$	4	4	$\tilde{4}$	15	21	$\widetilde{22}$	85	88	94

M

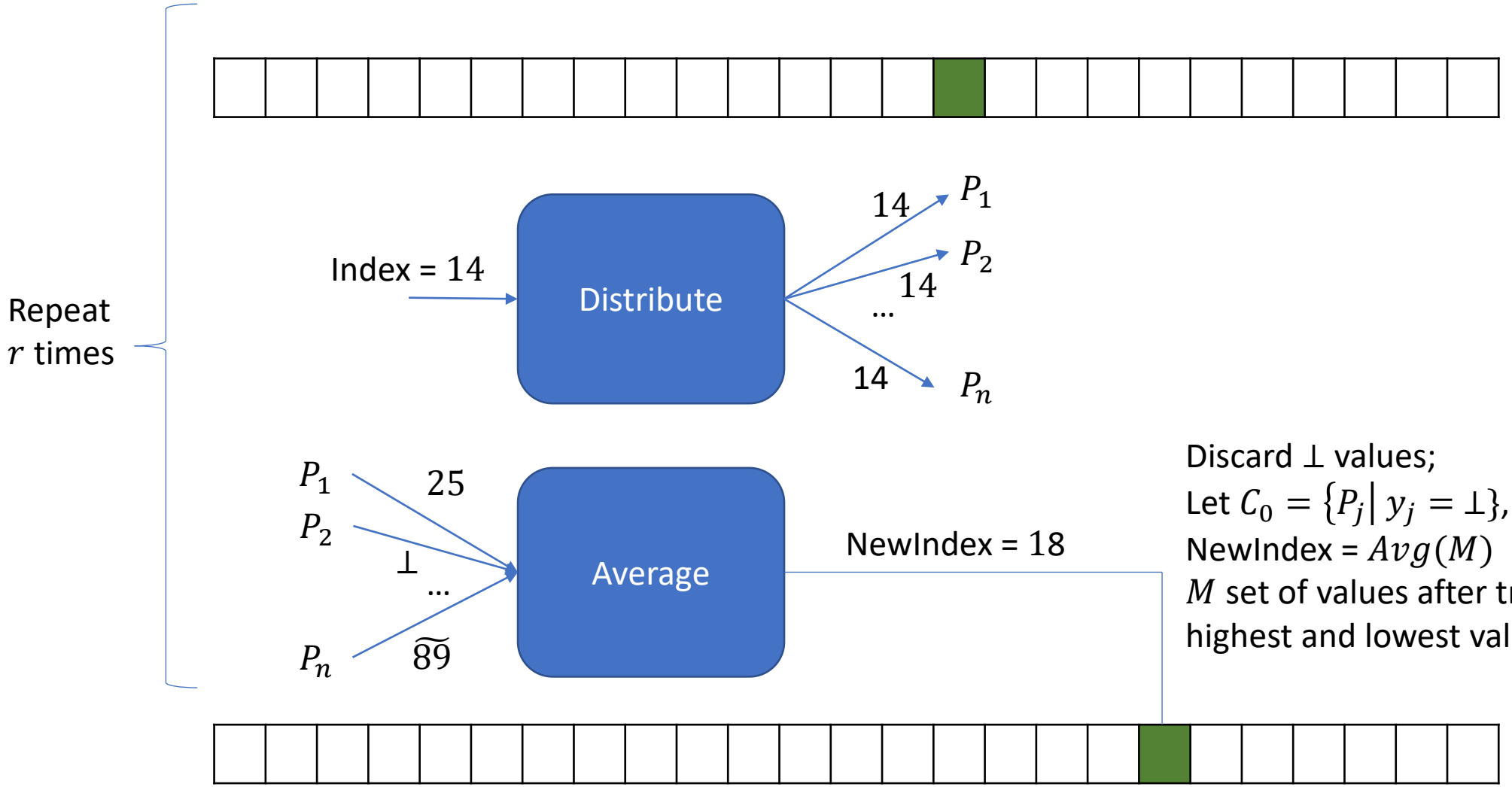
Update the corrupted set $C = C \cup C_0 \cup C_1$

Expansion with $\sim \mathbf{r}^{\mathbf{r}}$ slots in $\mathbf{3r}$ rounds



Discard $\perp$ values;
Let $C_0 = \{P_j | \, y_j = \perp\}$, $C_1 = \{P_j | \, y_j = \tilde{y}\}$
NewIndex = $Avg(M)$
M set of values after trimming $t - |C_0|$ highest and lowest values of non-$\perp$ values

Expansion with $\sim \mathbf{r}^{\mathbf{r}}$ slots in $\mathbf{3r}$ rounds



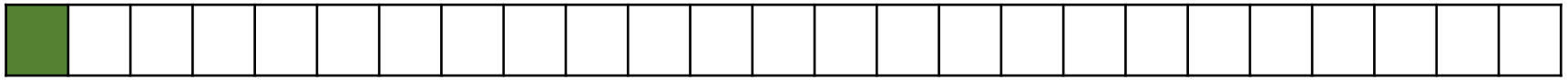
Discard $\perp$ values;
Let $C_0 = \{P_j | \, y_j = \perp\}$, $C_1 = \{P_j | \, y_j = \tilde{y}\}$
NewIndex = $Avg(M)$
M set of values after trimming $t - |C_0|$ highest and lowest values of non-$\perp$ values

Validity

$x_i = 0$ for all honest P_i

Averaging mechanism ensures that the new output is within the range of honest indices

…



Distribute + Average

Local set C of recognized corrupted parties

P_i dishonest

Index = x

Distribute

P_1 | y | $\tilde{y}$ | $\perp$ | $\tilde{*}$ | $*$

P_2 | y | $\tilde{y}$ | $\perp$ | $\tilde{*}$ | $*$

...

P_n | y | $\tilde{y}$ | $\perp$ | $\tilde{*}$ | $*$

P_1 $y_1 = \tilde{5}$

P_2 9

...

P_n $\perp$

Average

Discard $\perp$ values, let $C_0 = \{P_j | \, y_j = \perp\}$, $C_1 = \{P_j | \, y_j = \tilde{y}\}$

NewIndex = $Avg(M)$

M set of values after trimming $t - |C_0|$ highest and lowest values of non-$\perp$ values

Difference in honest sets M occurs when P_i sends | y | $\tilde{y}$ | $\perp$ | $\tilde{*}$ | $*$ |

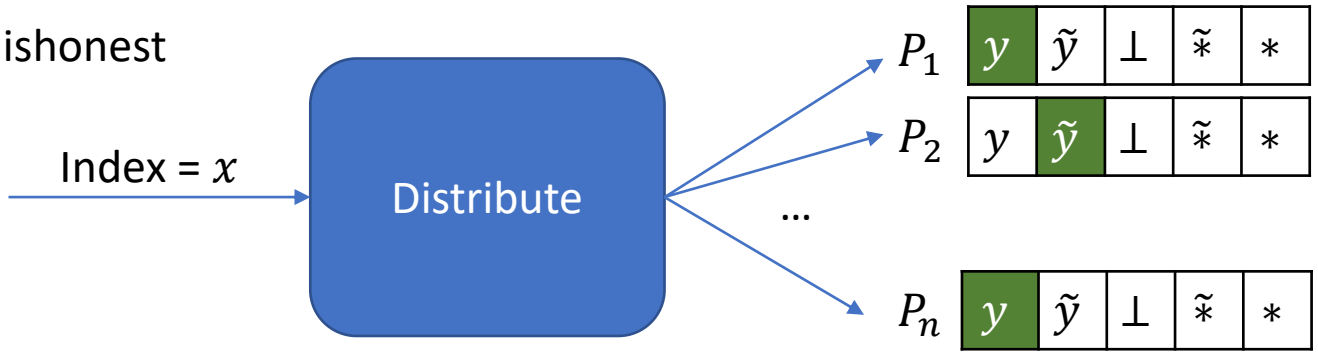
Update the corrupted set $C = C \cup C_0 \cup C_1$

Limiting Cheating

Local set C of recognized corrupted parties

P_i dishonest

Index = x



Discard $\perp$ values, let $C_0 = \{P_j | \, y_j = \perp\}$, $C_1 = \{P_j | \, y_j = \tilde{y}\}$

NewIndex = $Avg(M)$

M set of values after trimming $t - |C_0|$ highest and lowest values of non-$\perp$ values

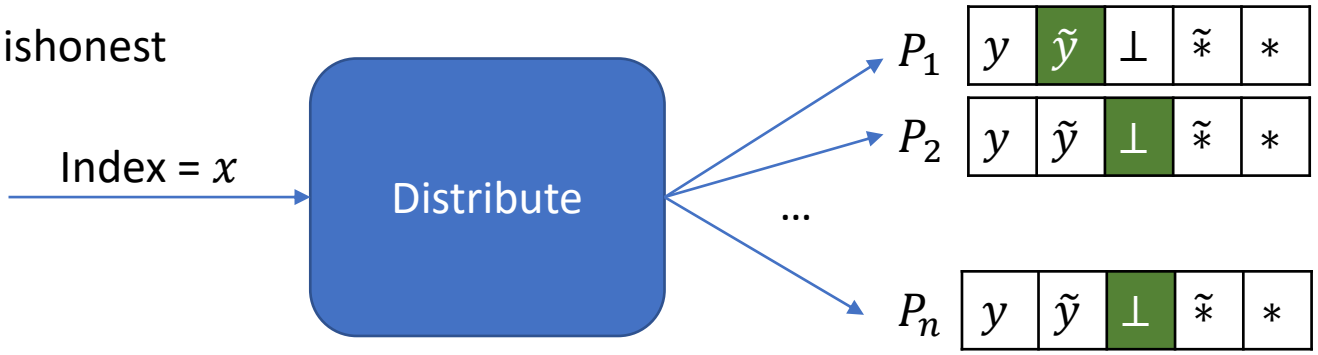
Update the corrupted set $C = C \cup C_0 \cup C_1$

Limiting Cheating

Local set C of recognized corrupted parties

P_i dishonest

Index = x



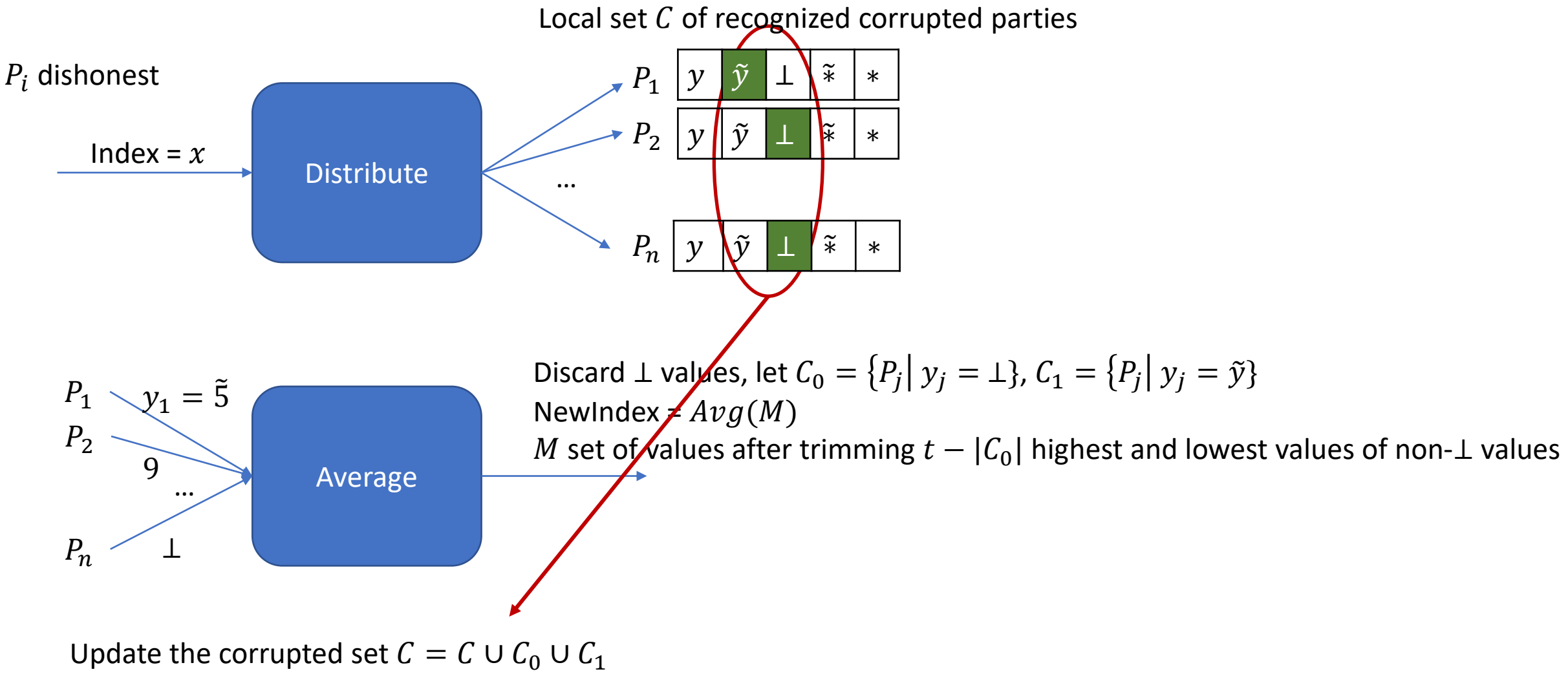
Discard $\perp$ values, let $C_0 = \{P_j | \, y_j = \perp\}$, $C_1 = \{P_j | \, y_j = \tilde{y}\}$

NewIndex = $Avg(M)$

M set of values after trimming $t - |C_0|$ highest and lowest values of non-$\perp$ values

Update the corrupted set $C = C \cup C_0 \cup C_1$

Limiting Cheating



Limiting Cheating

Local set C of recognized corrupted parties

P_i dishonest

Index = x

Distribute

P_1	y	$\tilde{y}$	$\perp$	$\tilde{*}$	$*$
P_2	y	$\tilde{y}$	$\perp$	$\tilde{*}$	$*$
...					
P_n	y	$\tilde{y}$	$\perp$	$\tilde{*}$	$*$

P_i is identified by all honest parties
⇒ all honest parties output $\perp$

P_1 $y_1 = \tilde{5}$
P_2 9
...
P_n $\perp$

Average

Discard $\perp$ values, let $C_0 = \{P_j | \, y_j = \perp\}$, $C_1 = \{P_j | \, y_j = \tilde{y}\}$
NewIndex = $Avg(M)$
M set of values after trimming $t - |C_0|$ highest and lowest values of non-$\perp$ values

Update the corrupted set $C = C \cup C_0 \cup C_1$

Limiting Cheating

Local set C of recognized corrupted parties

P_i dishonest

Index = x

Distribute

P_1	y	$\tilde{y}$	$\perp$	$\tilde{*}$	$*$
P_2	y	$\tilde{y}$	$\perp$	$\tilde{*}$	$*$
...					
P_n	y	$\tilde{y}$	$\perp$	$\tilde{*}$	$*$

P_i is identified by all honest parties
⇒ all honest parties output $\perp$

P_1 $y_1 = \tilde{5}$
P_2 9
...
P_n $\perp$

Average

Discard $\perp$ values, let $C_0 = \{P_j | \, y_j = \perp\}$, $C_1 = \{P_j | \, y_j = \tilde{y}\}$
NewIndex = $Avg(M)$
M set of values after trimming $t - |C_0|$ highest and lowest values of non-$\perp$ values

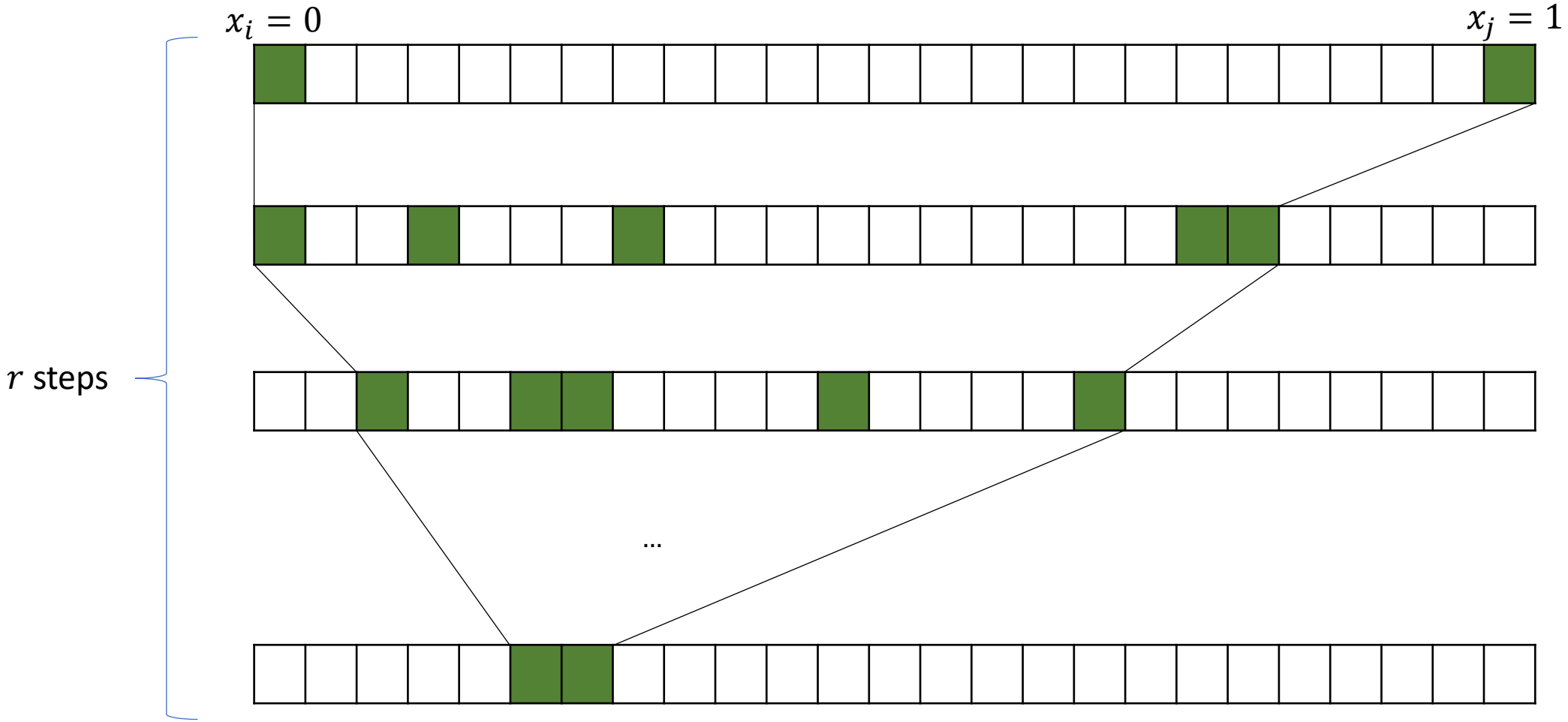
Difference in honest sets M occurs when
P_i sends

y	$\tilde{y}$	$\perp$	$\tilde{*}$	$*$

Only happens once!

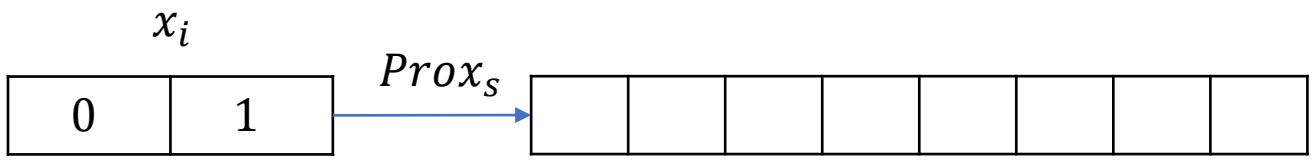
Update the corrupted set $C = C \cup C_0 \cup C_1$

Consistency

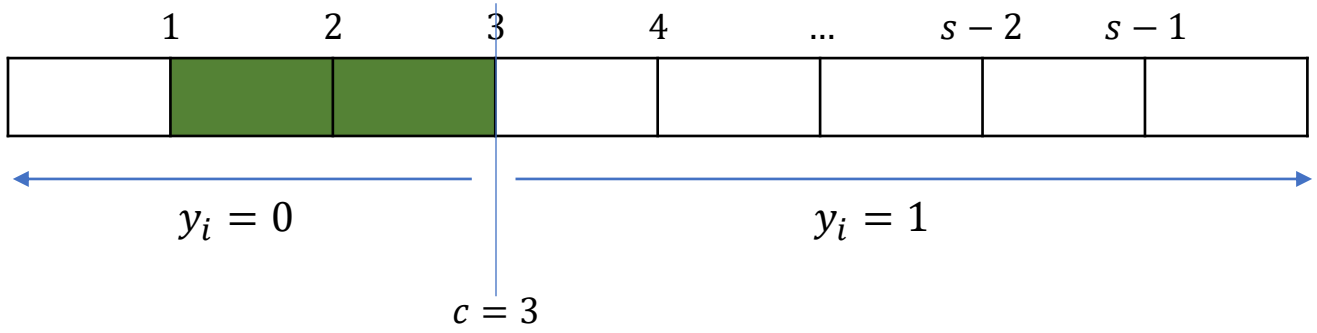


Honest interval shrinks by $1/r$ at each step (on average)

Expand-and-Extract



Each P_i gets a common random $c \leftarrow_{\$} \{1, s-1\}$



Set $x_i = y_i$

Validity

If ∀ honest P_i inputs $x_i = x \in \{0,1\}$,
then no matter the coin value,
it holds that $y_i = x$

Consistency

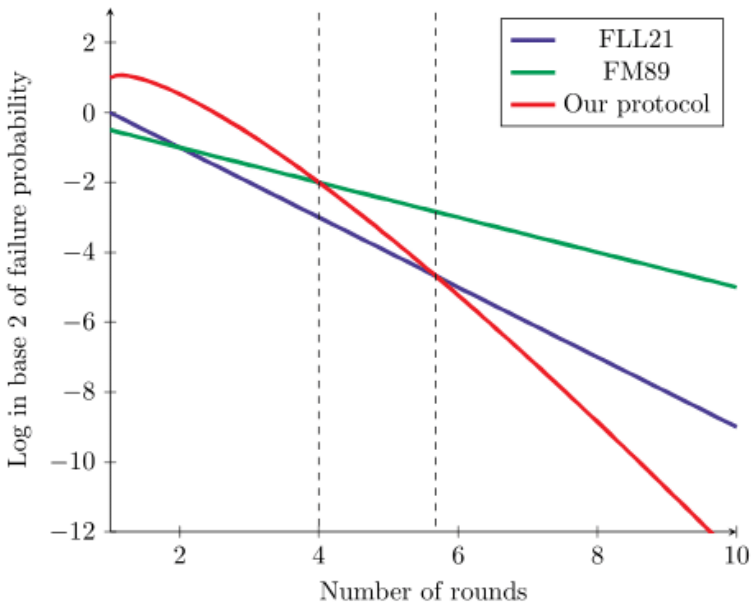
Only one coin value causes disagreement

$\Pr[agree] \geq 1 - \frac{1}{s-1}$

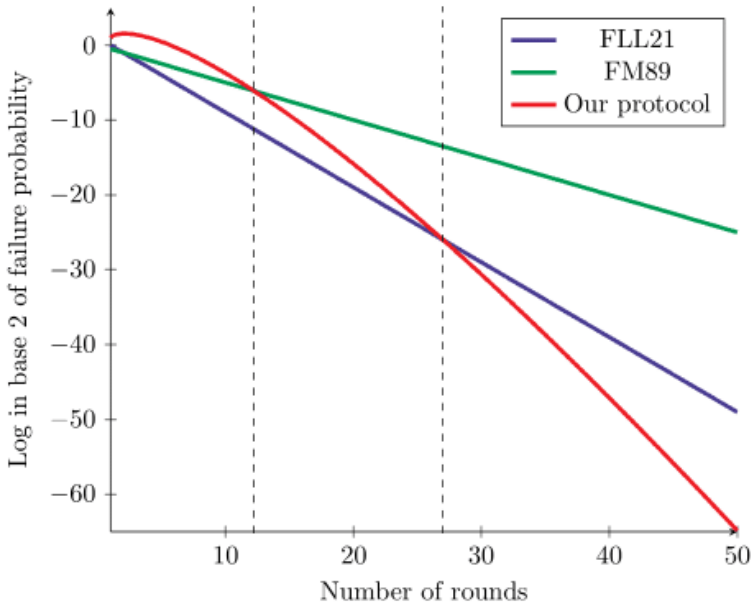
$\boldsymbol{s \sim r^r}$

$O(r)$ rounds: agreement with probability $1 - \frac{1}{r^r}$

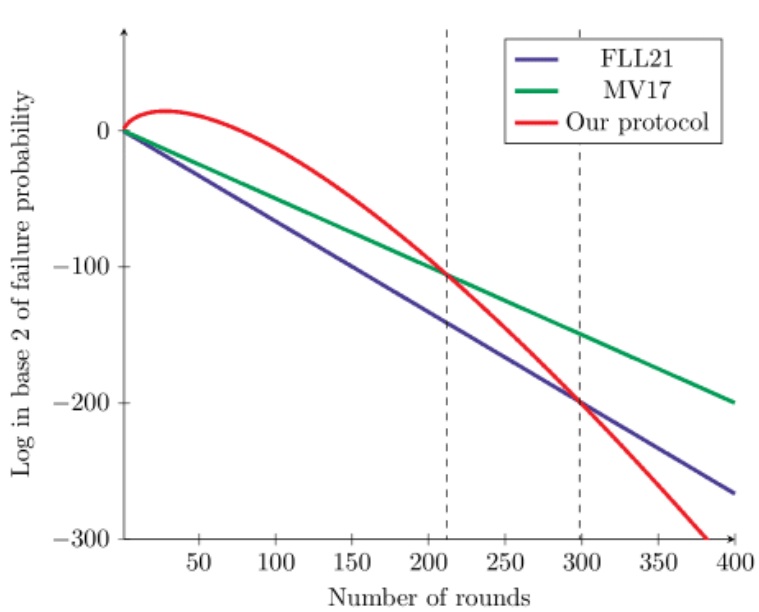
Some Numbers



(a) $t < n/10$
The failure probability of our protocol becomes lower than that of [FM89] after 4 iterations, and lower than that of [FLL21] after 6 iterations.



(b) $t < n/3$
The failure probability of our protocol becomes lower than that of [FM89] after 13 iterations, and lower than that of [FLL21] after 27 iterations.



(c) $t < 0.49 \cdot n$
The failure probability of our protocol becomes lower than that of [MV17] after 212 iterations, and lower than that of [FLL21] after 299 iterations.

Thank you!