Public Randomness Extraction with Ephemeral Roles and Worst-Case Corruptions

Jesper Buus Nielsen
Aarhus

João Ribeiro
CMU

Maciej Obremski
CQT & NUS

Cryptography needs randomness!

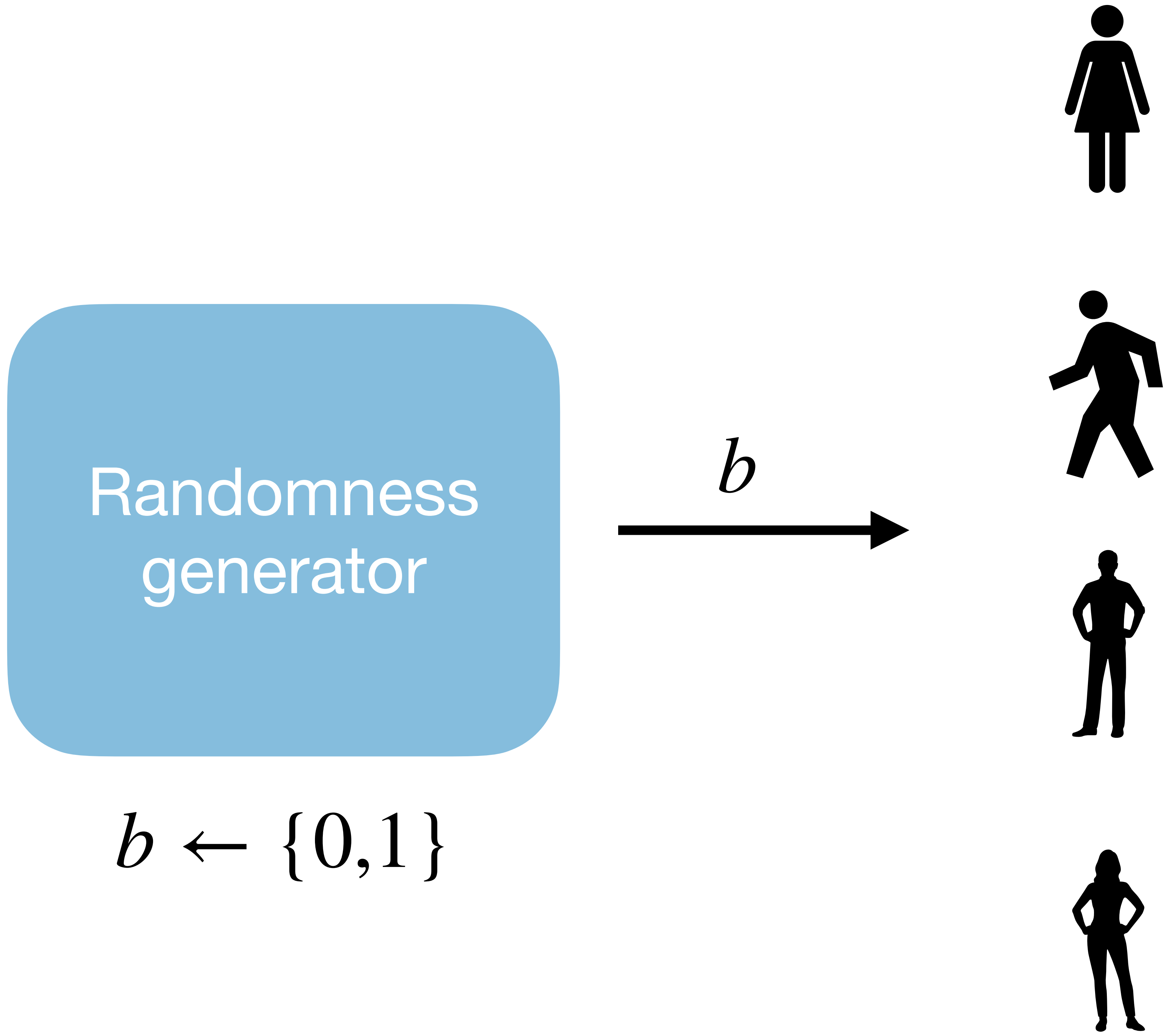
How do we generate it?

Cryptography needs randomness!

How do we generate it?

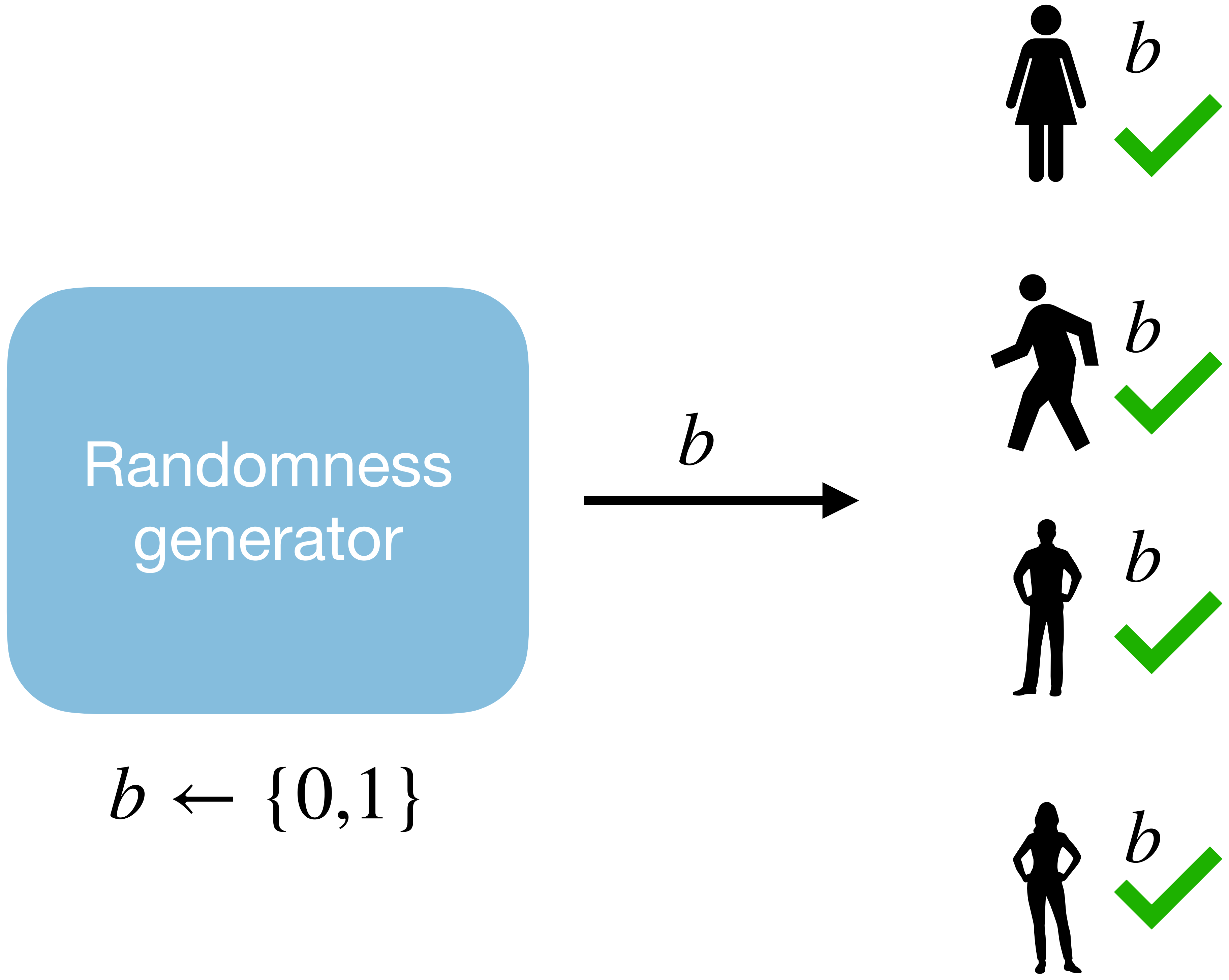
Cryptography needs randomness!

How do we generate it?



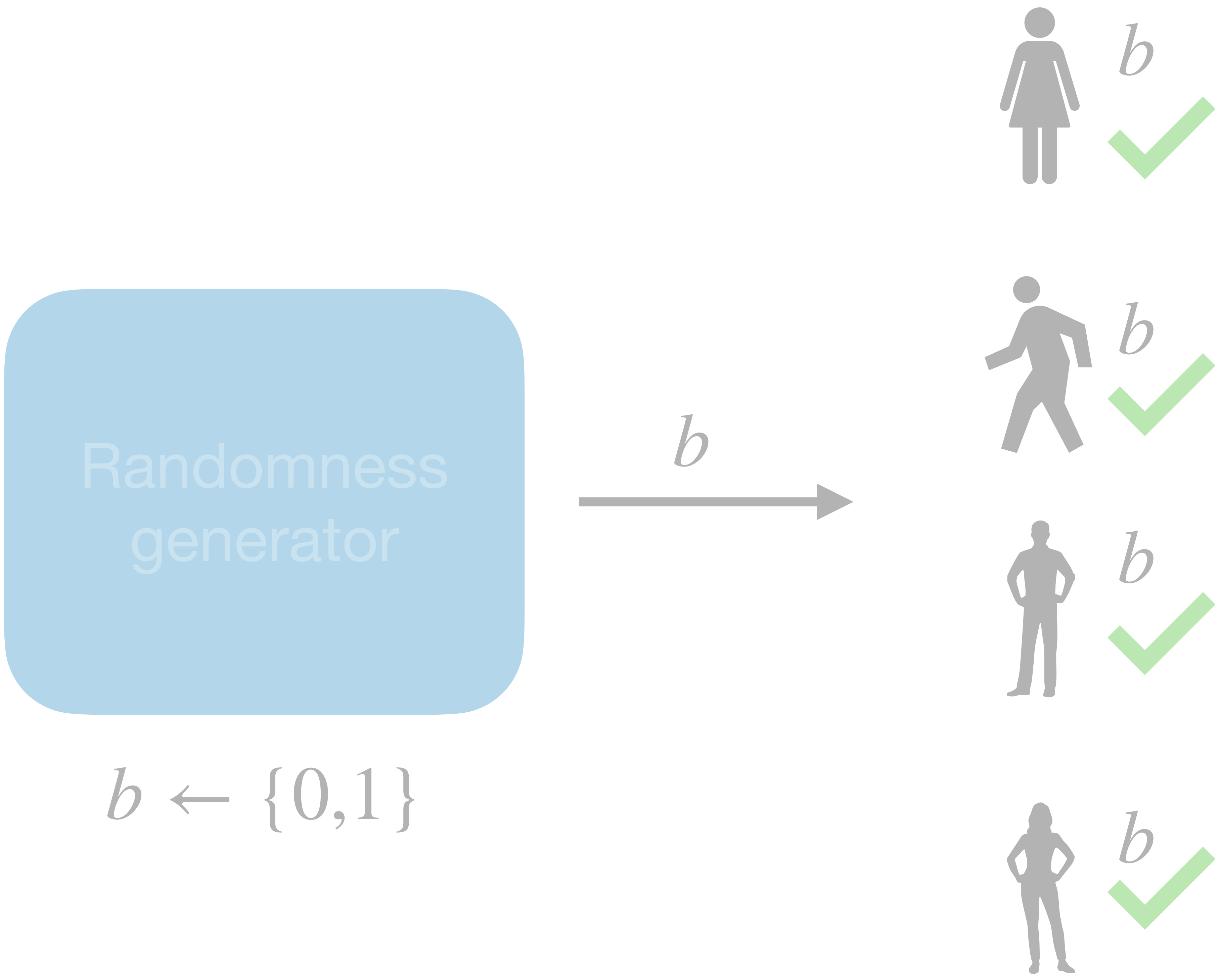
Cryptography needs randomness!

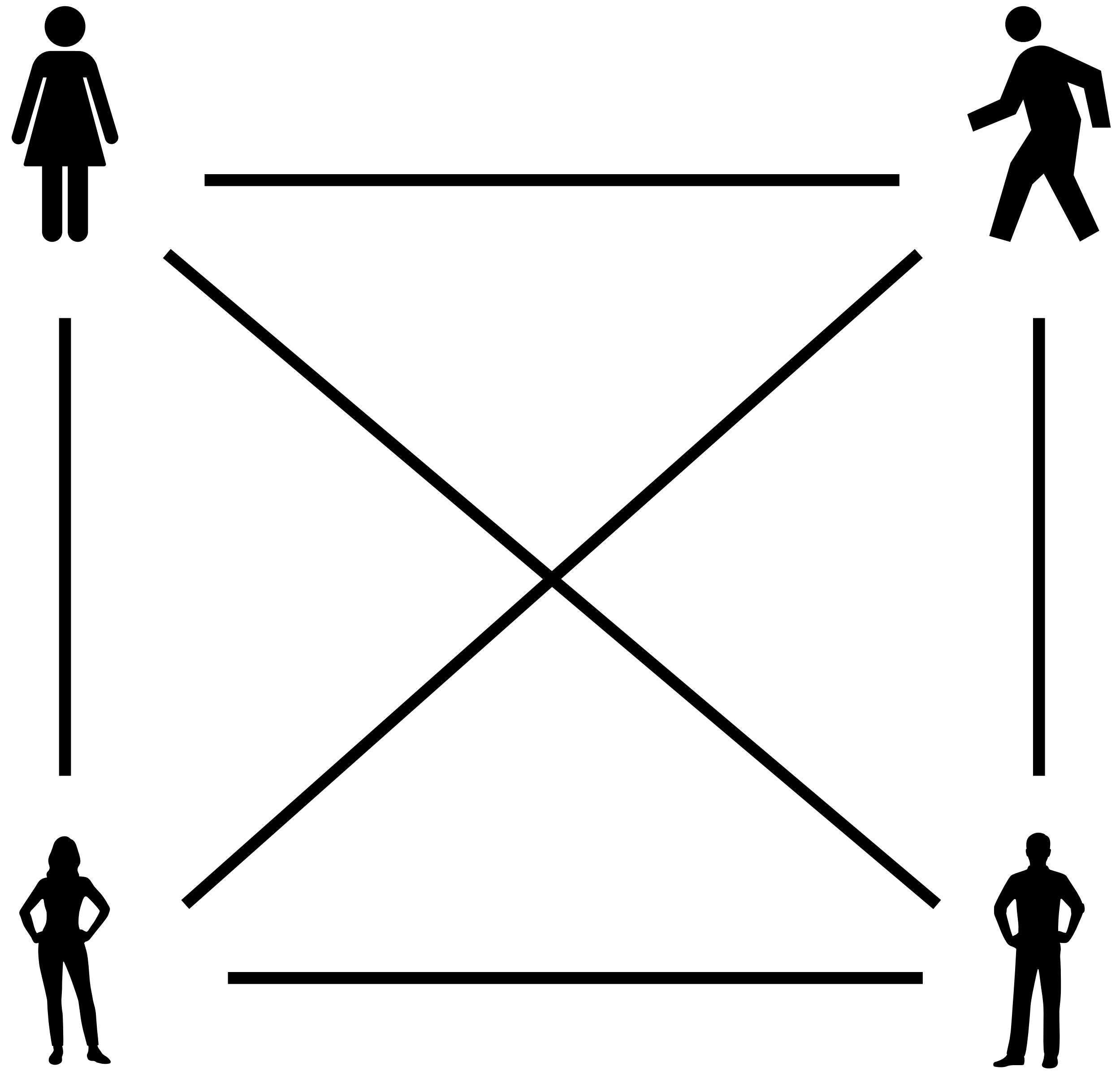
How do we generate it?



Cryptography needs randomness!

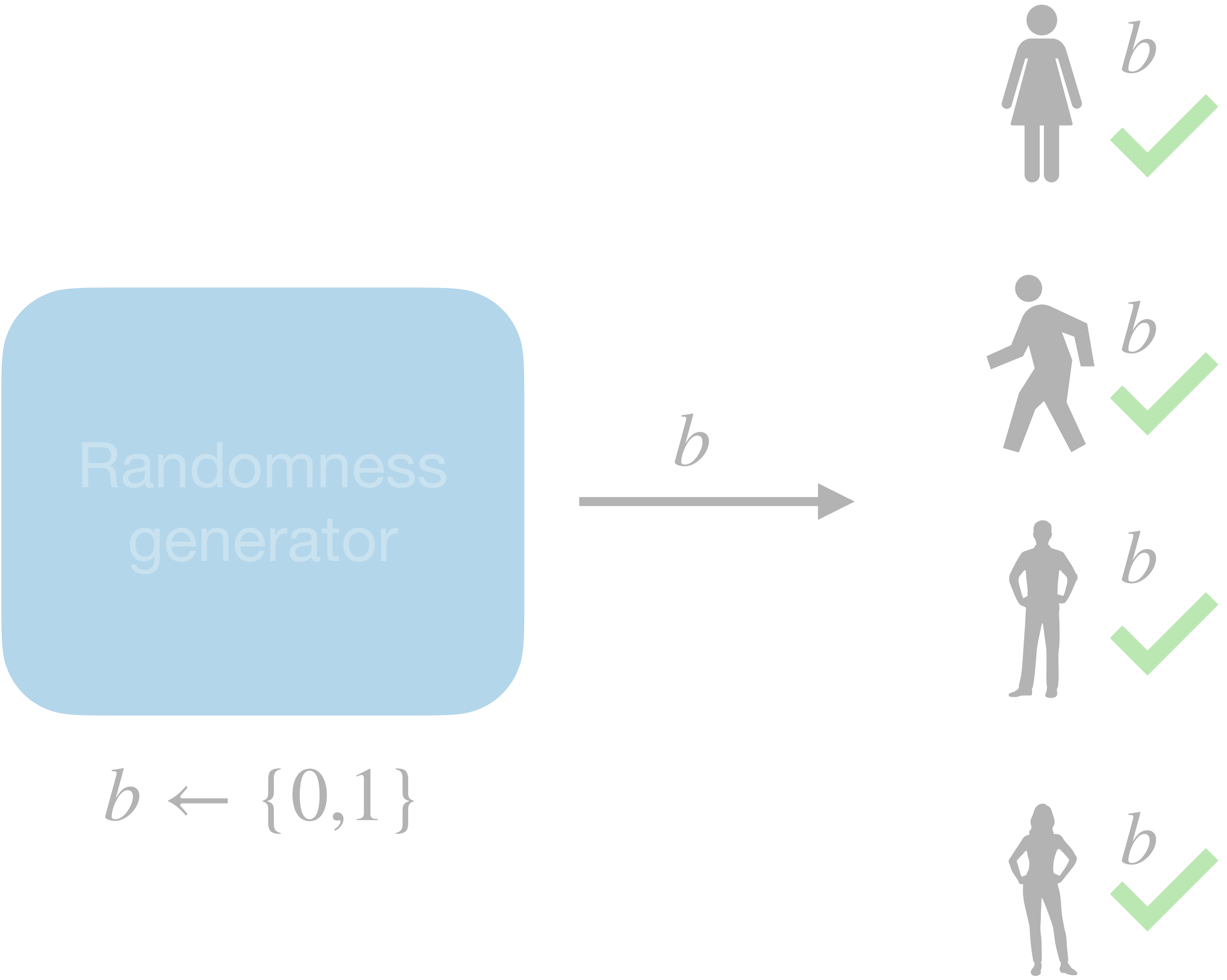
How do we generate it?

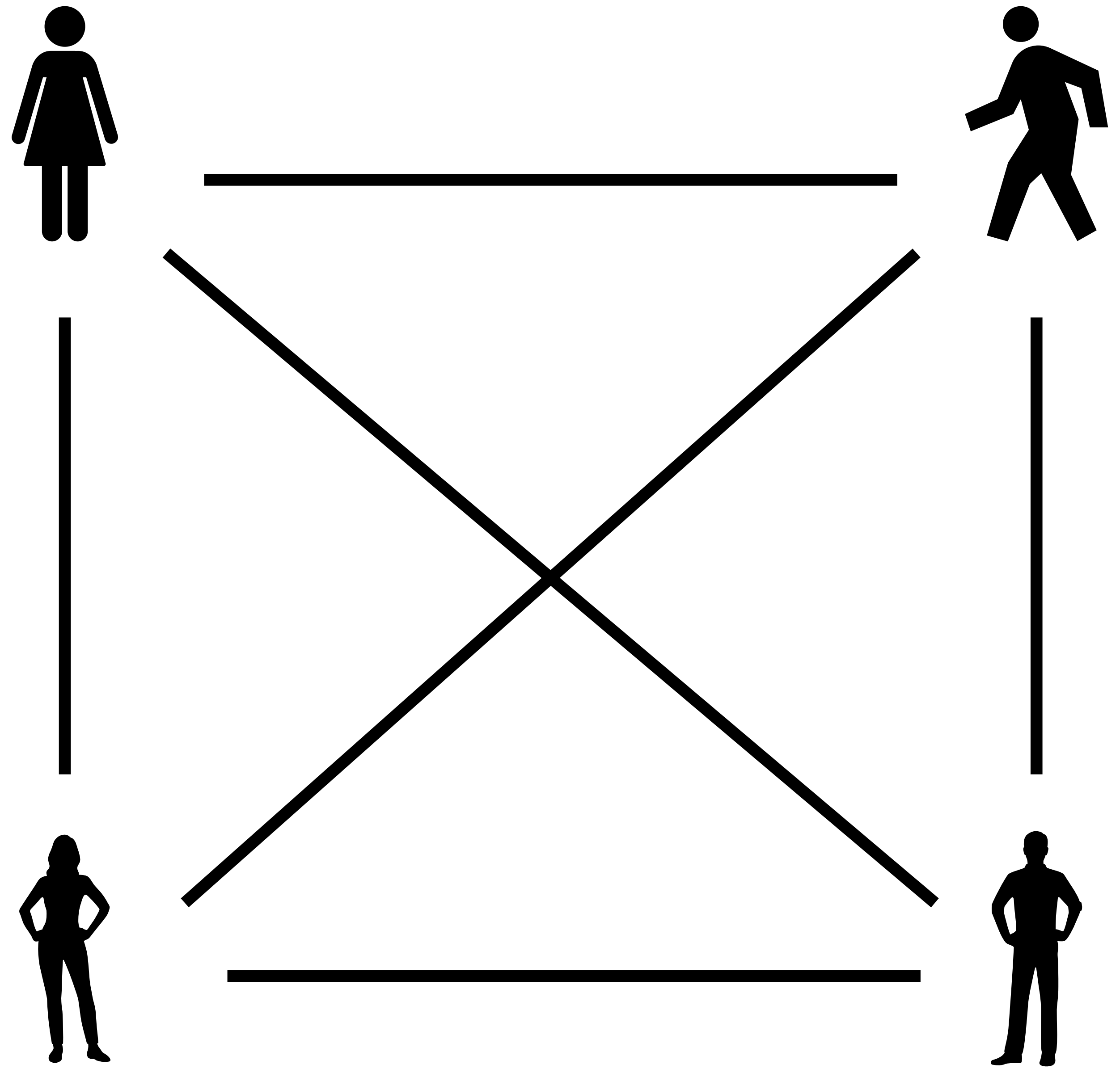




Cryptography needs randomness!

How do we generate it?

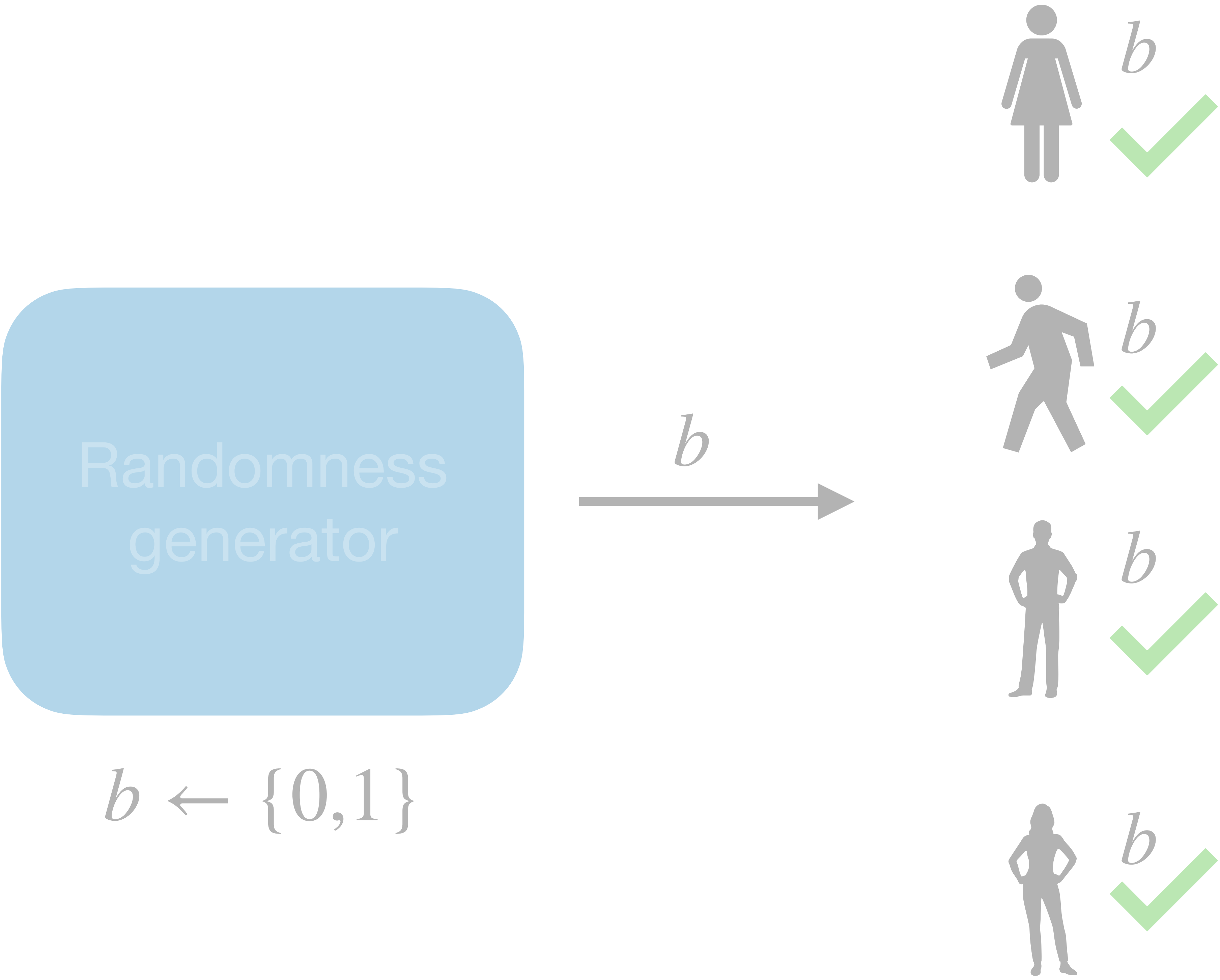


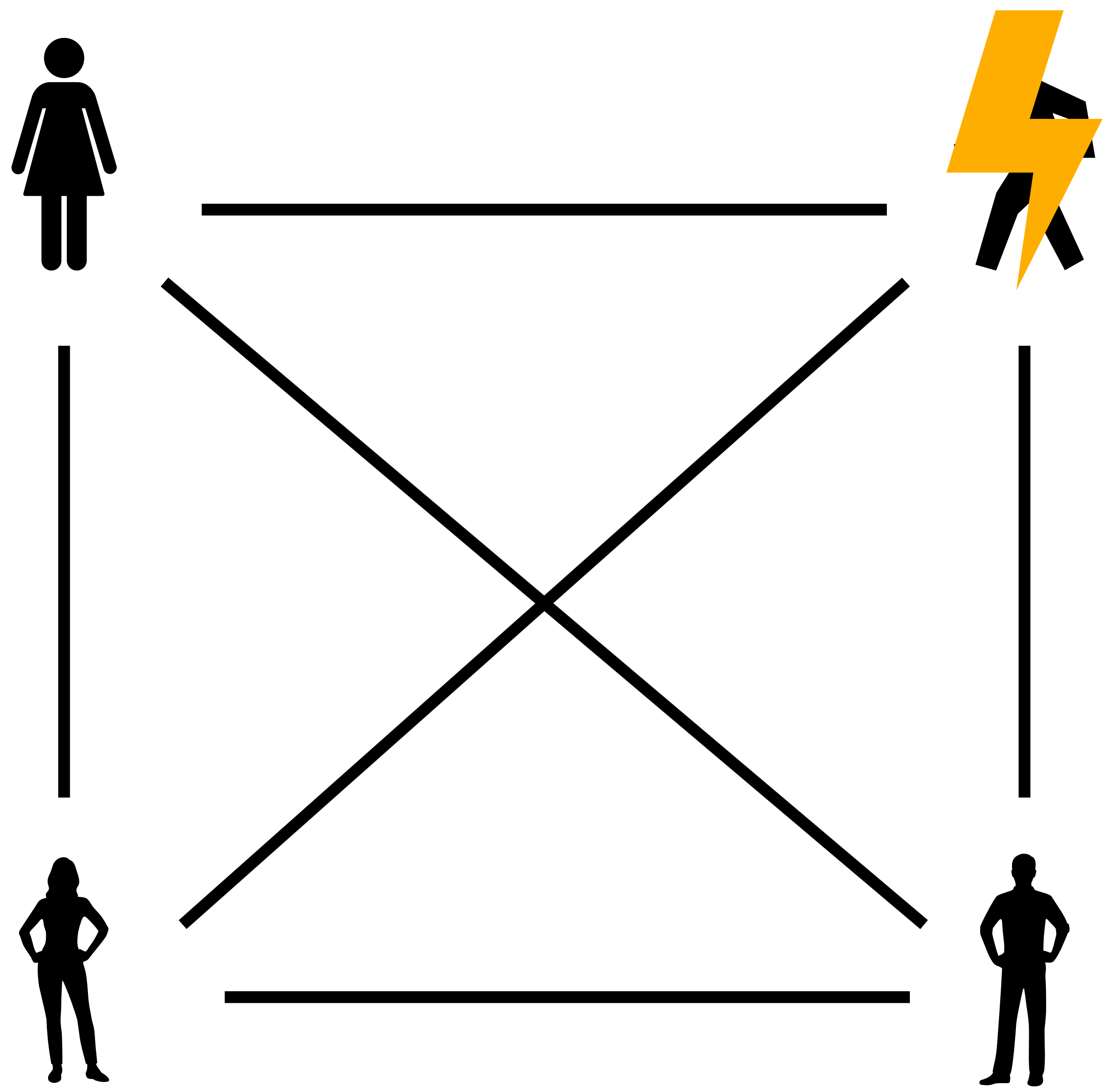


but maintaining stateful environments is hard, especially under targeted denial-of-service attacks!

Cryptography needs randomness!

How do we generate it?

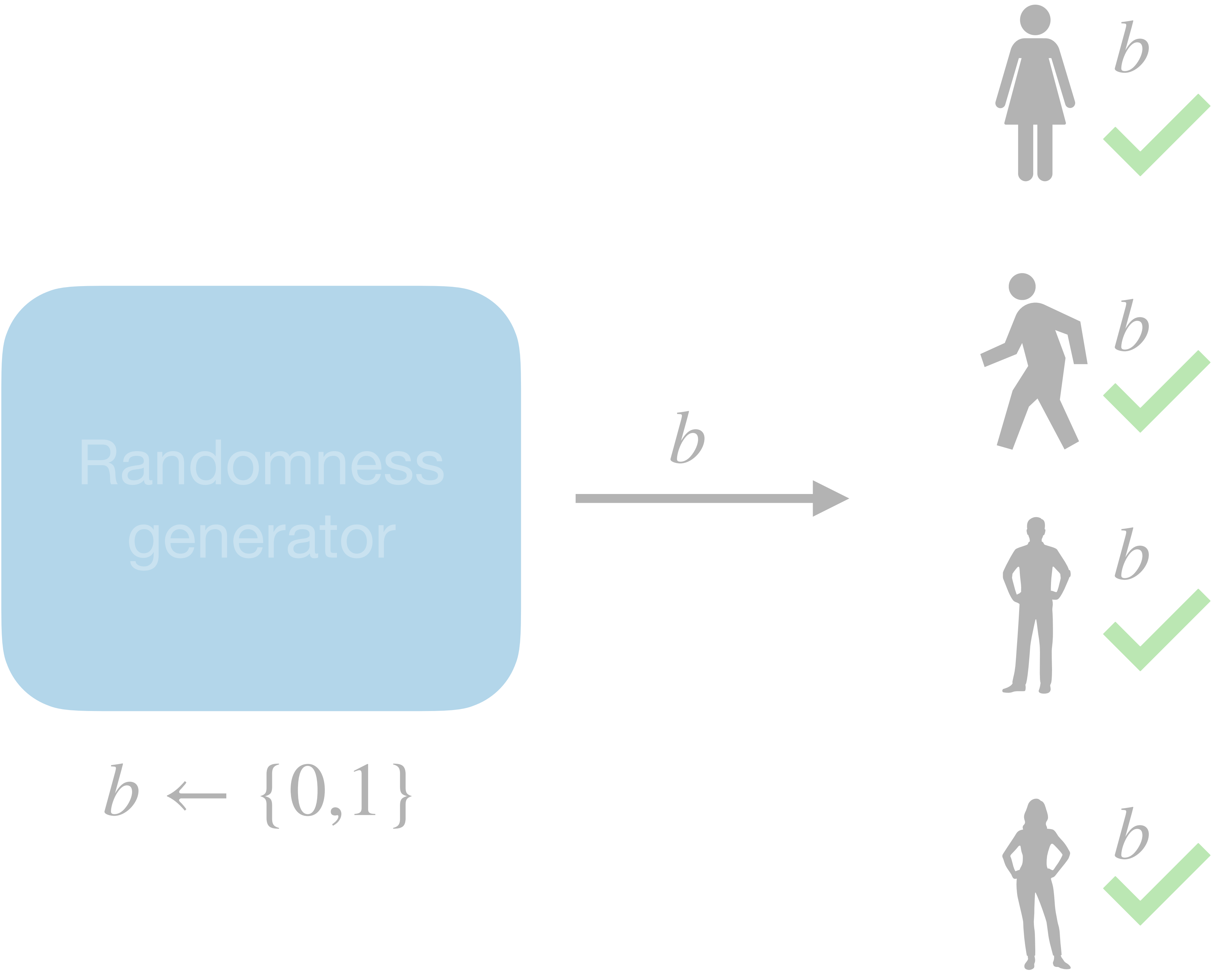


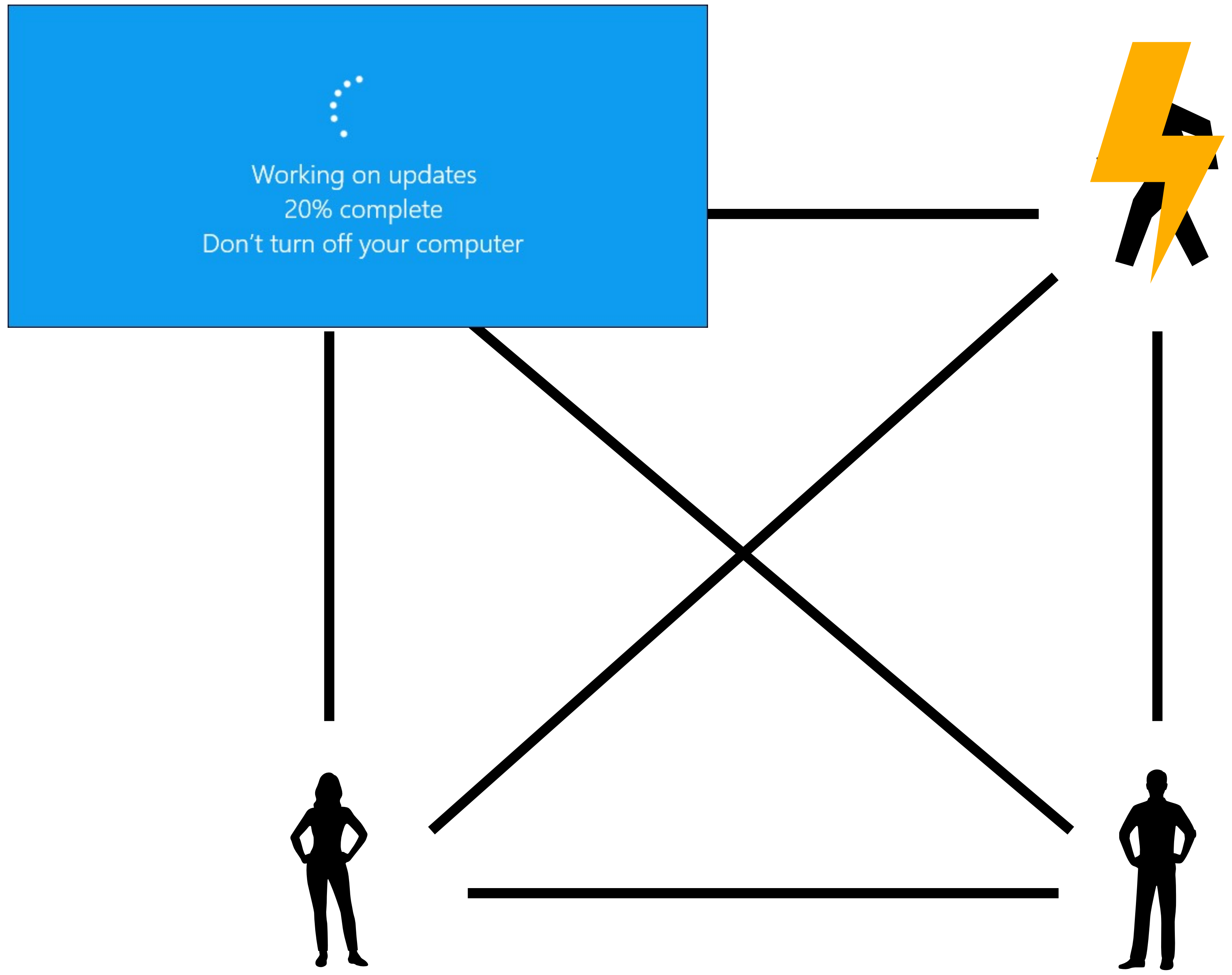


but maintaining stateful environments is hard, especially under targeted denial-of-service attacks!

Cryptography needs randomness!

How do we generate it?





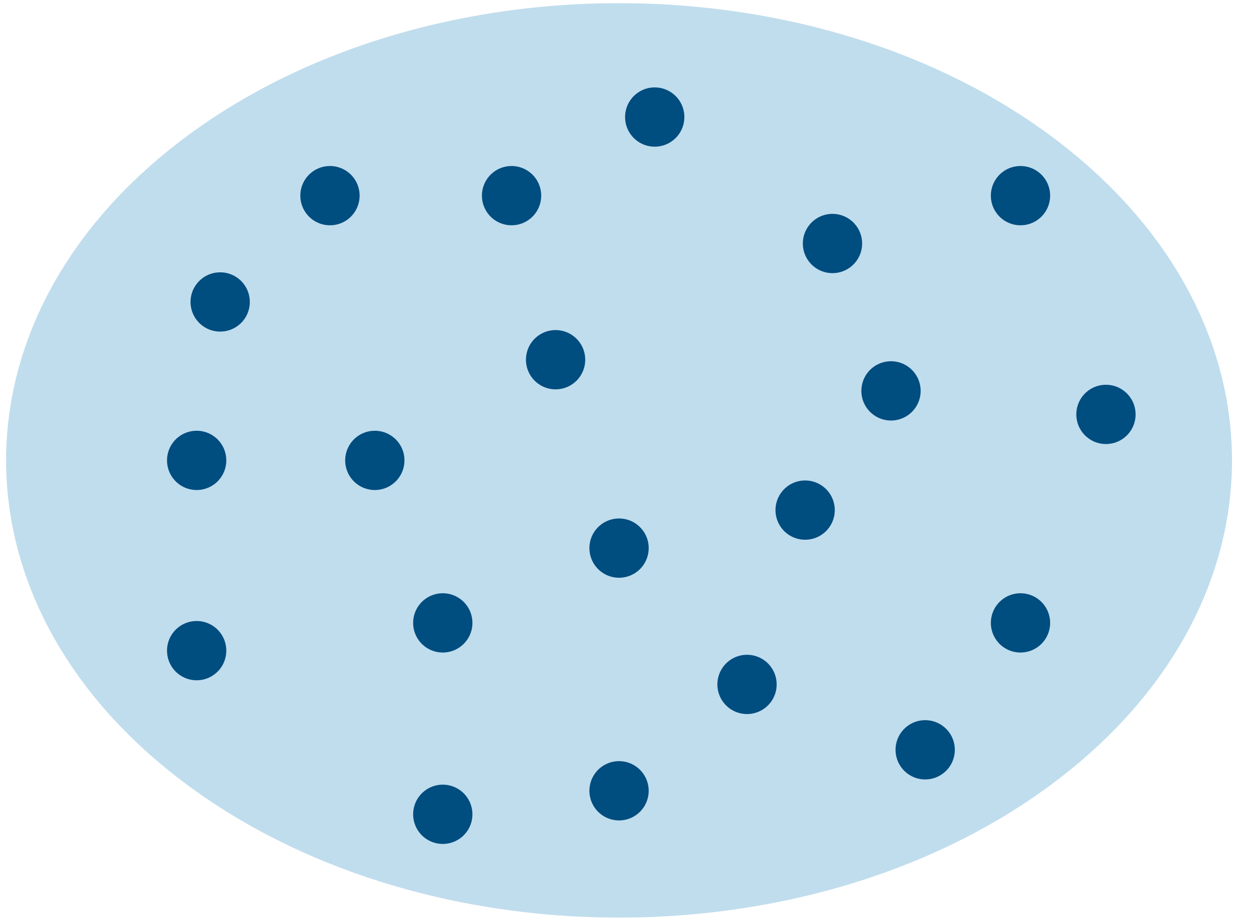
but maintaining stateful environments is hard, especially under targeted denial-of-service attacks!

YOSO: You Only Speak Once

Secure MPC with Stateless Ephemeral Roles

Craig Gentry[1], Shai Halevi[1], Hugo Krawczyk[1], Bernardo Magri[2], Jesper Buus Nielsen[*2], Tal Rabin[1], and Sophia Yakoubov[†3]

Ground set of N parties



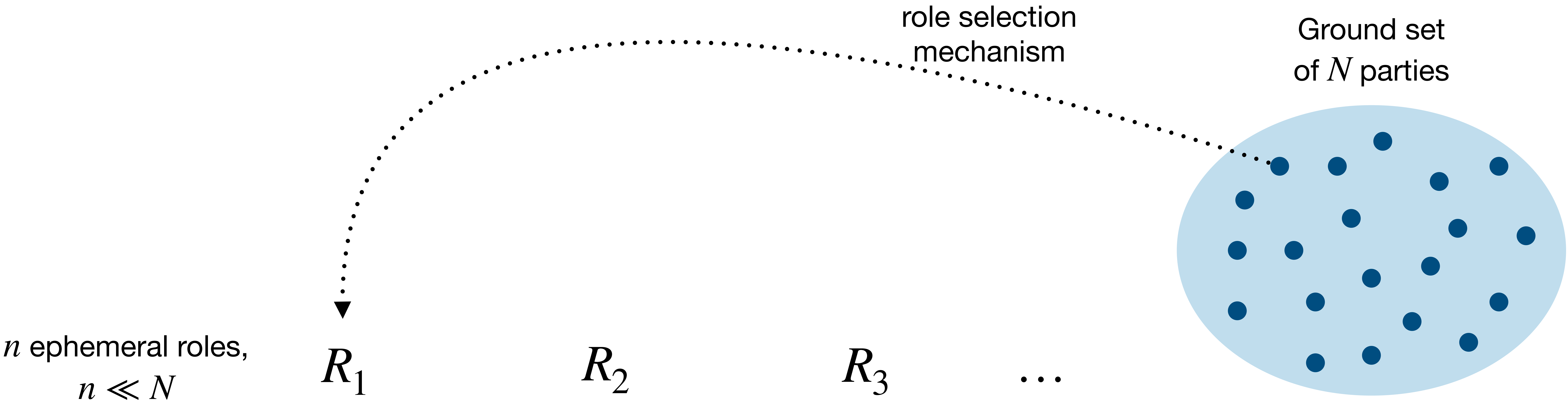
n ephemeral roles, $n \ll N$

R_1 R_2 R_3 $\ldots$

YOSO: You Only Speak Once

Secure MPC with Stateless Ephemeral Roles

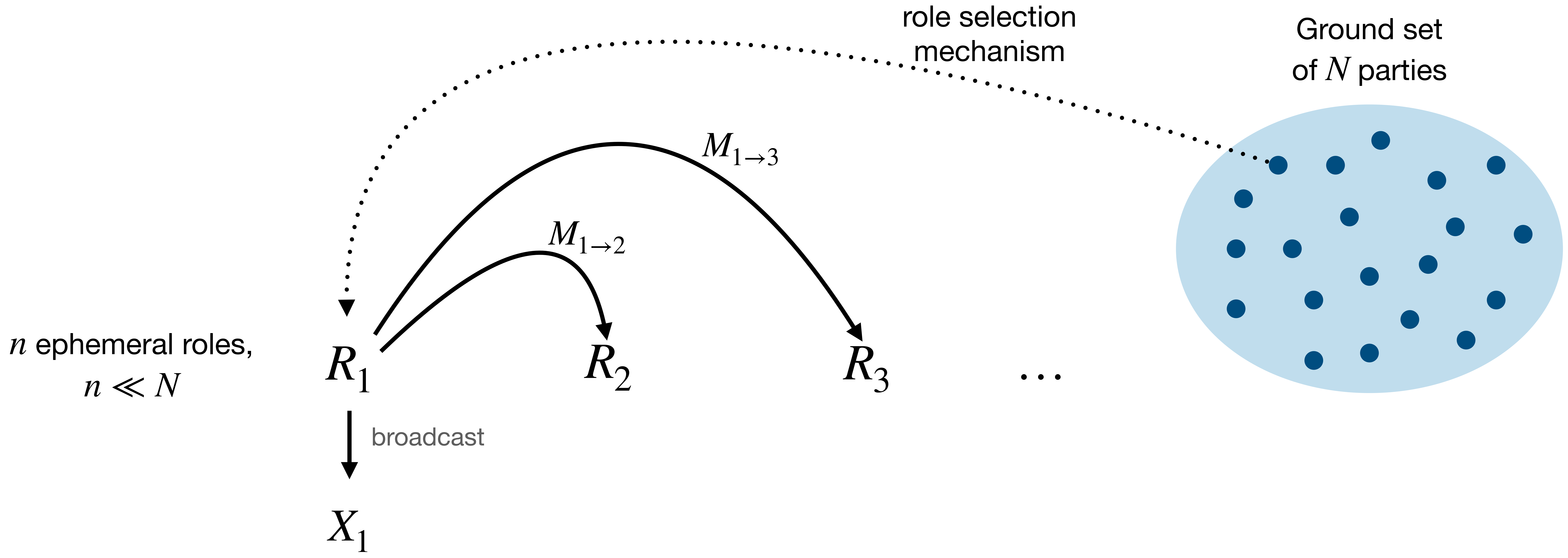
Craig Gentry[1], Shai Halevi[1], Hugo Krawczyk[1], Bernardo Magri[2], Jesper Buus Nielsen[*2], Tal Rabin[1], and Sophia Yakoubov[†3]

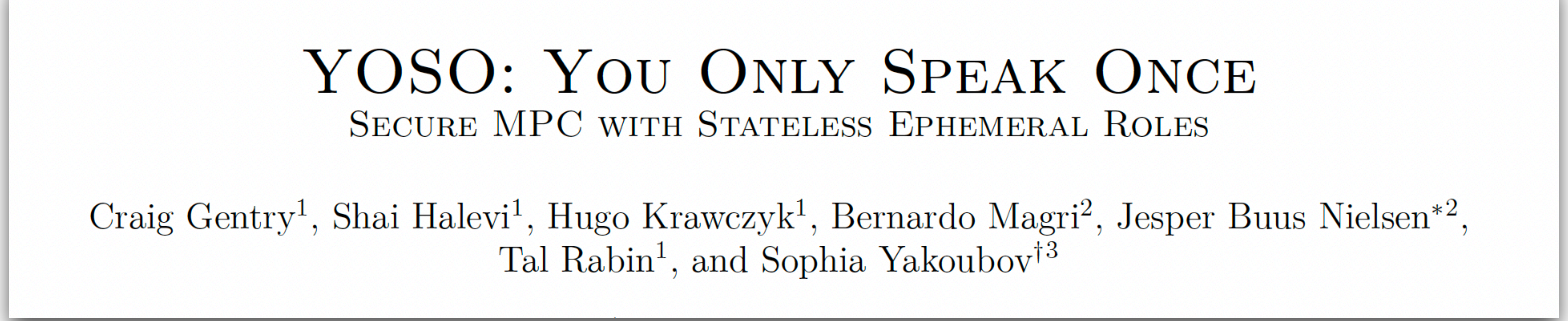


YOSO: You Only Speak Once

Secure MPC with Stateless Ephemeral Roles

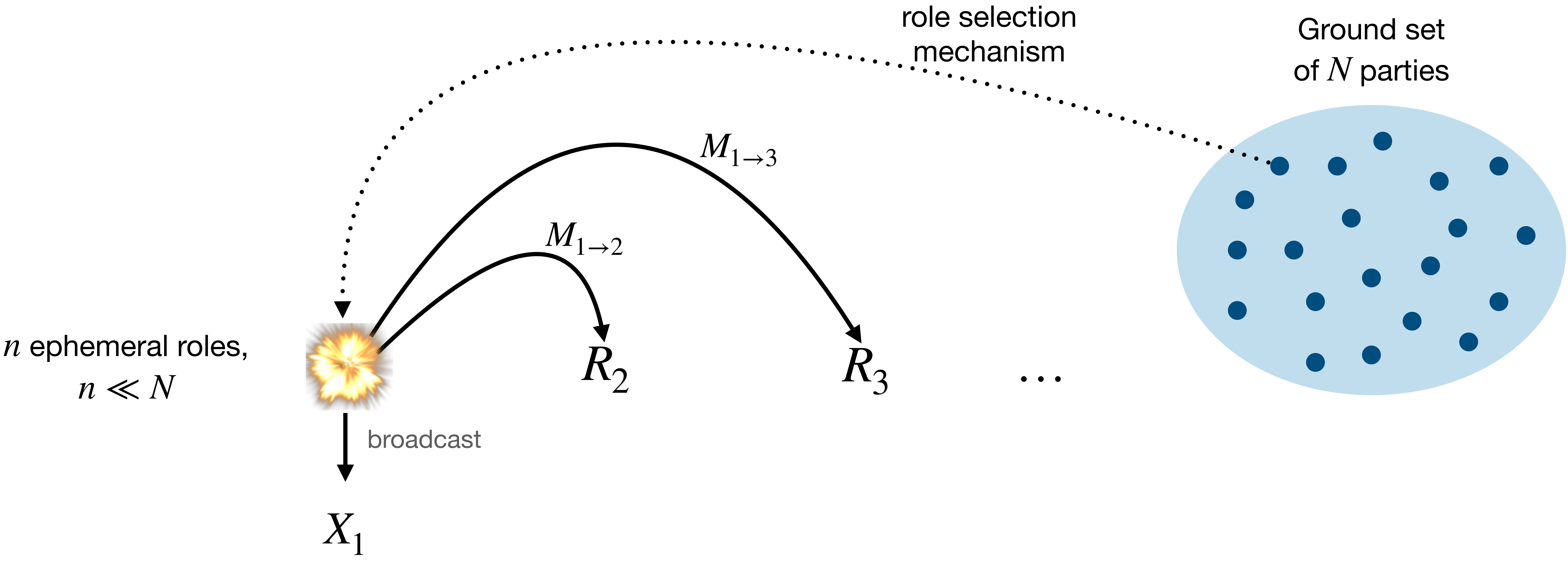
Craig Gentry[1], Shai Halevi[1], Hugo Krawczyk[1], Bernardo Magri[2], Jesper Buus Nielsen[*2], Tal Rabin[1], and Sophia Yakoubov[†3]





YOSO: You Only Speak Once
Secure MPC with Stateless Ephemeral Roles

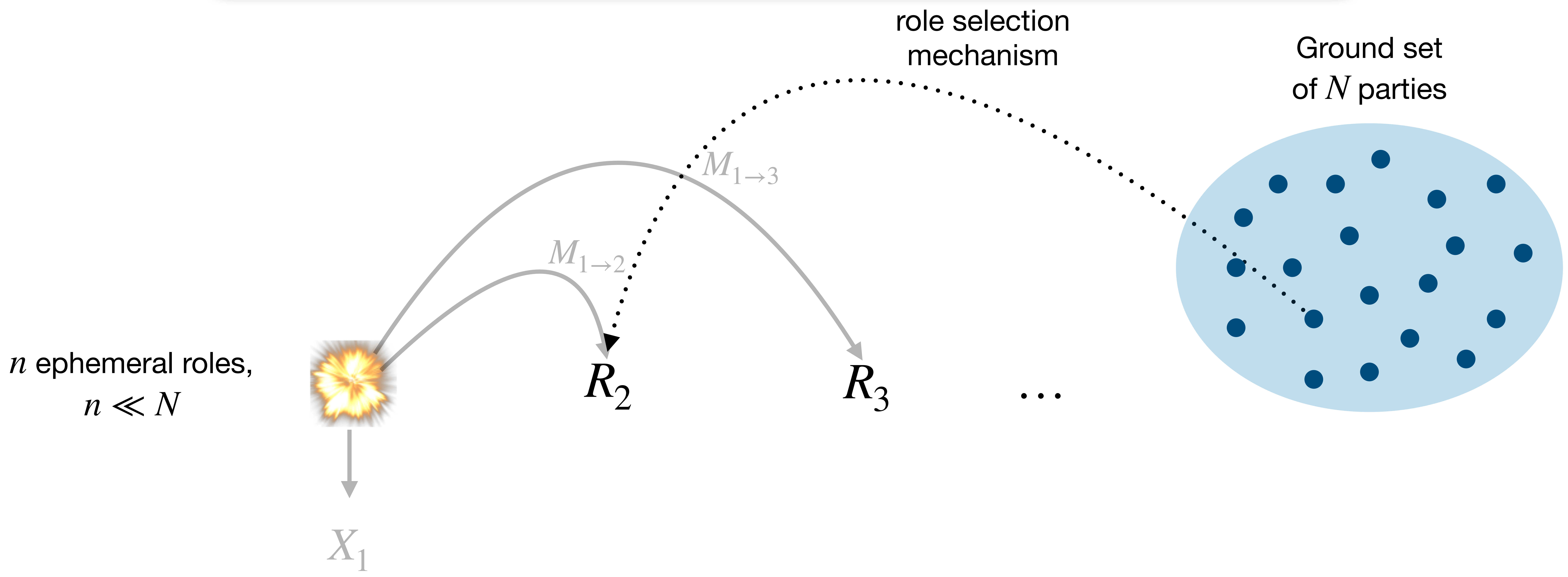
Craig Gentry[1], Shai Halevi[1], Hugo Krawczyk[1], Bernardo Magri[2], Jesper Buus Nielsen[*2], Tal Rabin[1], and Sophia Yakoubov[†3]



YOSO: You Only Speak Once

Secure MPC with Stateless Ephemeral Roles

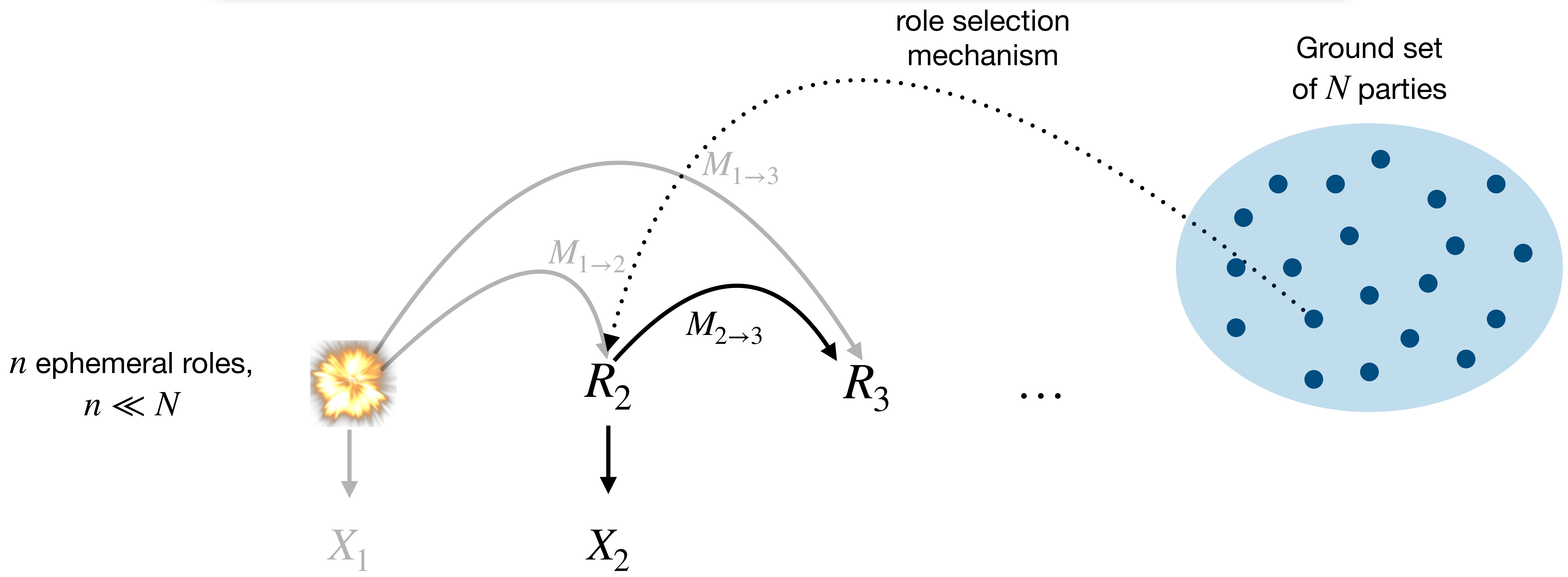
Craig Gentry[1], Shai Halevi[1], Hugo Krawczyk[1], Bernardo Magri[2], Jesper Buus Nielsen[*2],
Tal Rabin[1], and Sophia Yakoubov[†3]



YOSO: You Only Speak Once

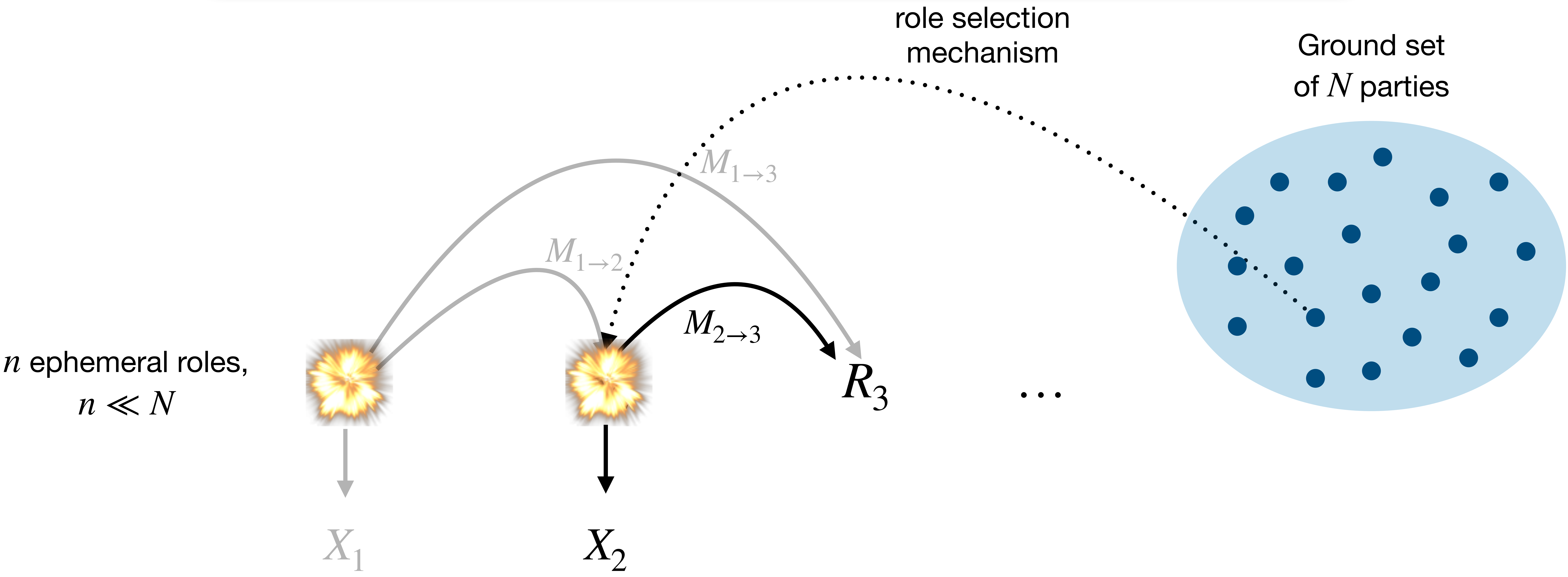
Secure MPC with Stateless Ephemeral Roles

Craig Gentry[1], Shai Halevi[1], Hugo Krawczyk[1], Bernardo Magri[2], Jesper Buus Nielsen[*2], Tal Rabin[1], and Sophia Yakoubov[†3]



YOSO: You Only Speak Once
Secure MPC with Stateless Ephemeral Roles

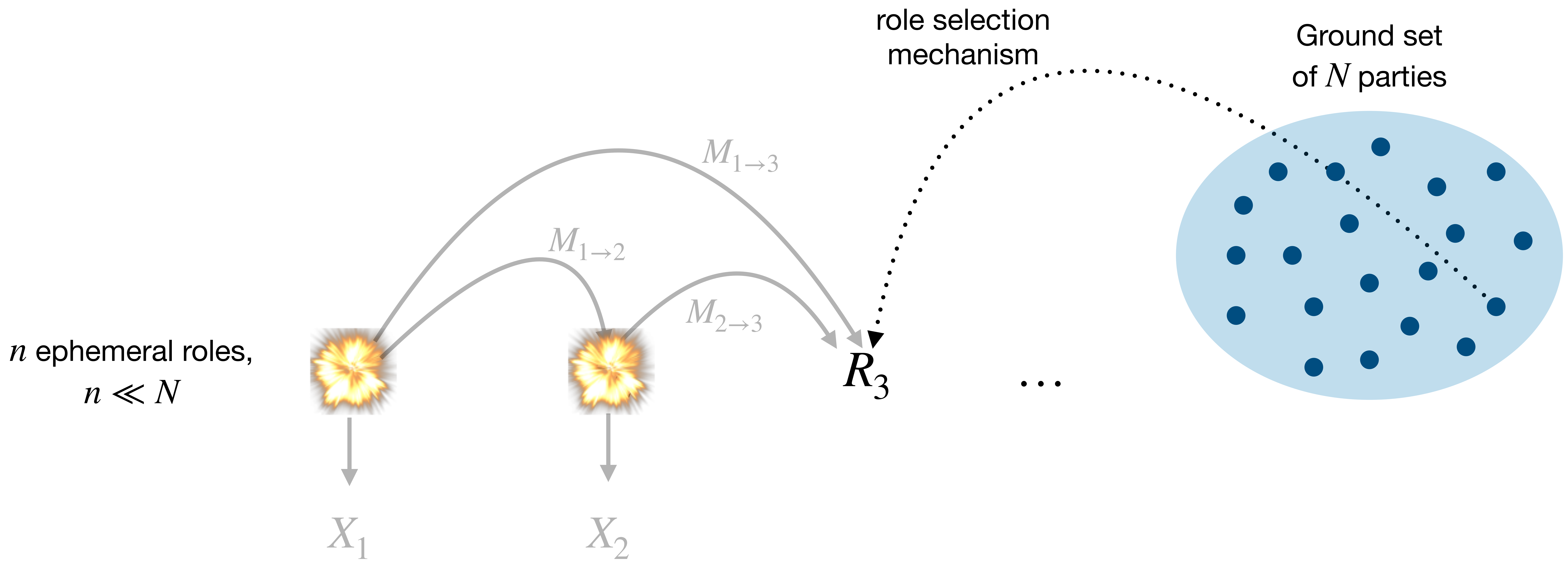
Craig Gentry[1], Shai Halevi[1], Hugo Krawczyk[1], Bernardo Magri[2], Jesper Buus Nielsen[*2], Tal Rabin[1], and Sophia Yakoubov[†3]



YOSO: You Only Speak Once

Secure MPC with Stateless Ephemeral Roles

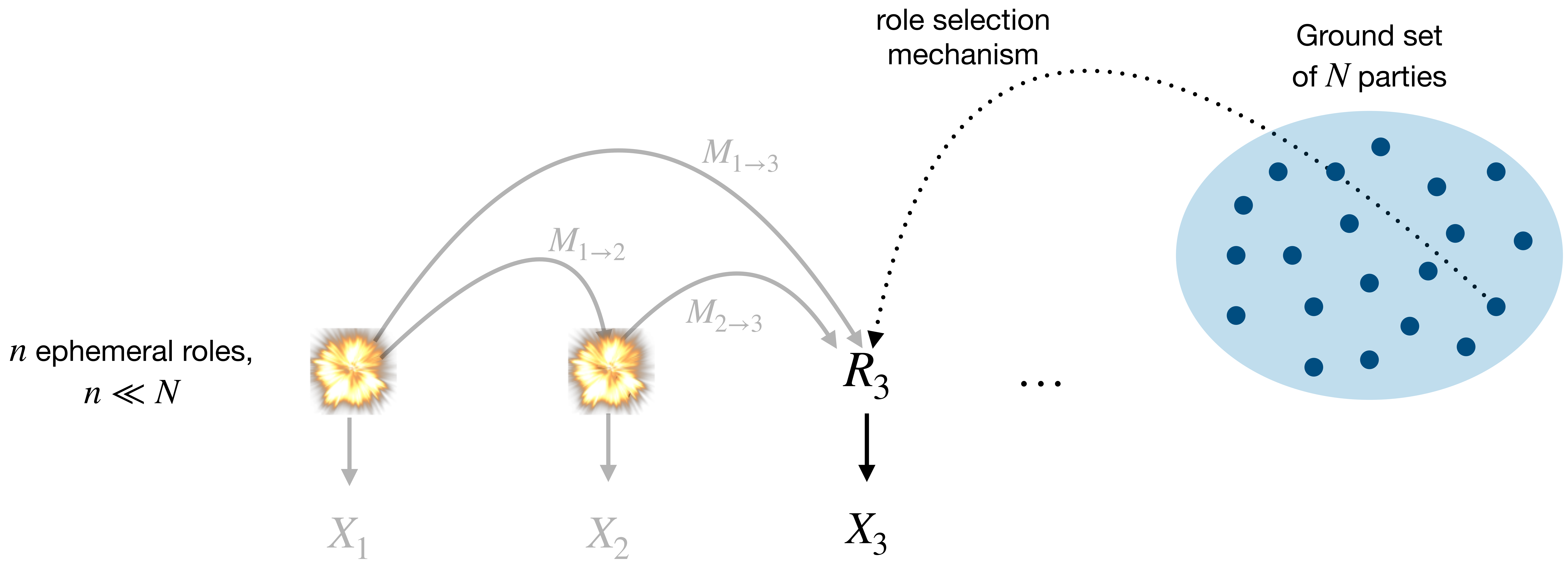
Craig Gentry[1], Shai Halevi[1], Hugo Krawczyk[1], Bernardo Magri[2], Jesper Buus Nielsen[*2], Tal Rabin[1], and Sophia Yakoubov[†3]



YOSO: You Only Speak Once

Secure MPC with Stateless Ephemeral Roles

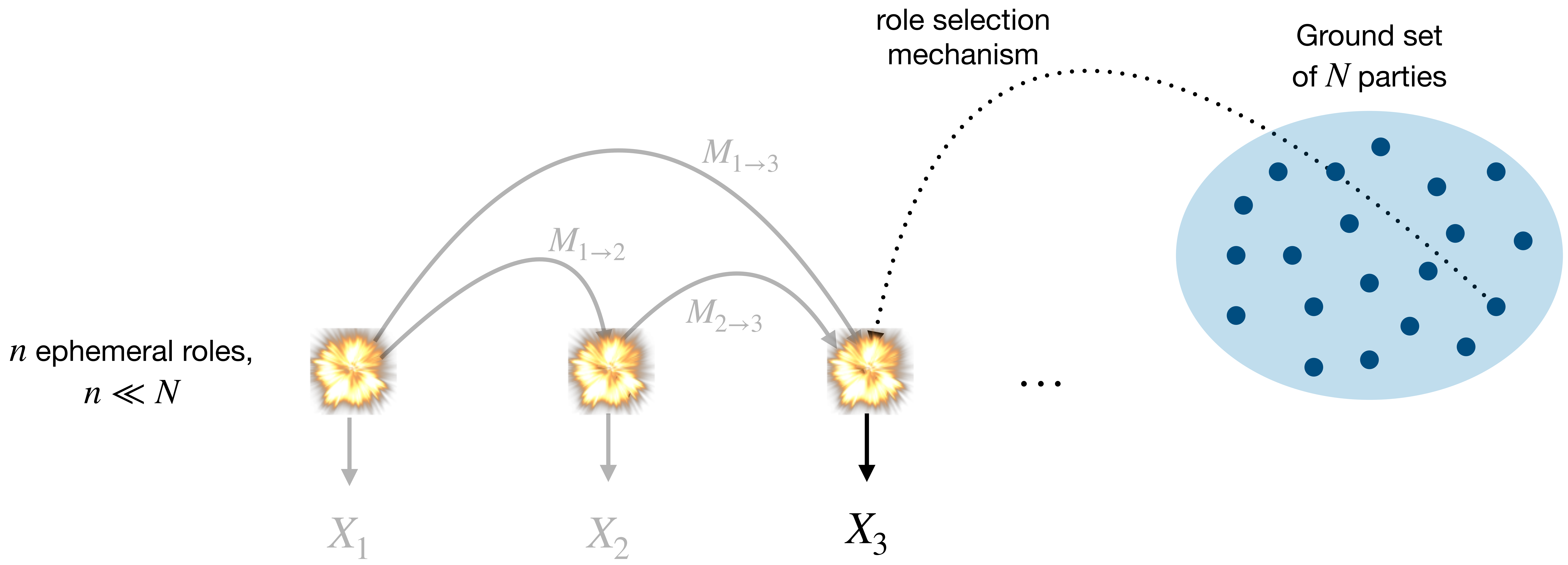
Craig Gentry[1], Shai Halevi[1], Hugo Krawczyk[1], Bernardo Magri[2], Jesper Buus Nielsen[*2], Tal Rabin[1], and Sophia Yakoubov[†3]



YOSO: You Only Speak Once

Secure MPC with Stateless Ephemeral Roles

Craig Gentry[1], Shai Halevi[1], Hugo Krawczyk[1], Bernardo Magri[2], Jesper Buus Nielsen[*2], Tal Rabin[1], and Sophia Yakoubov[†3]



YOSO: You Only Speak Once

Secure MPC with Stateless Ephemeral Roles

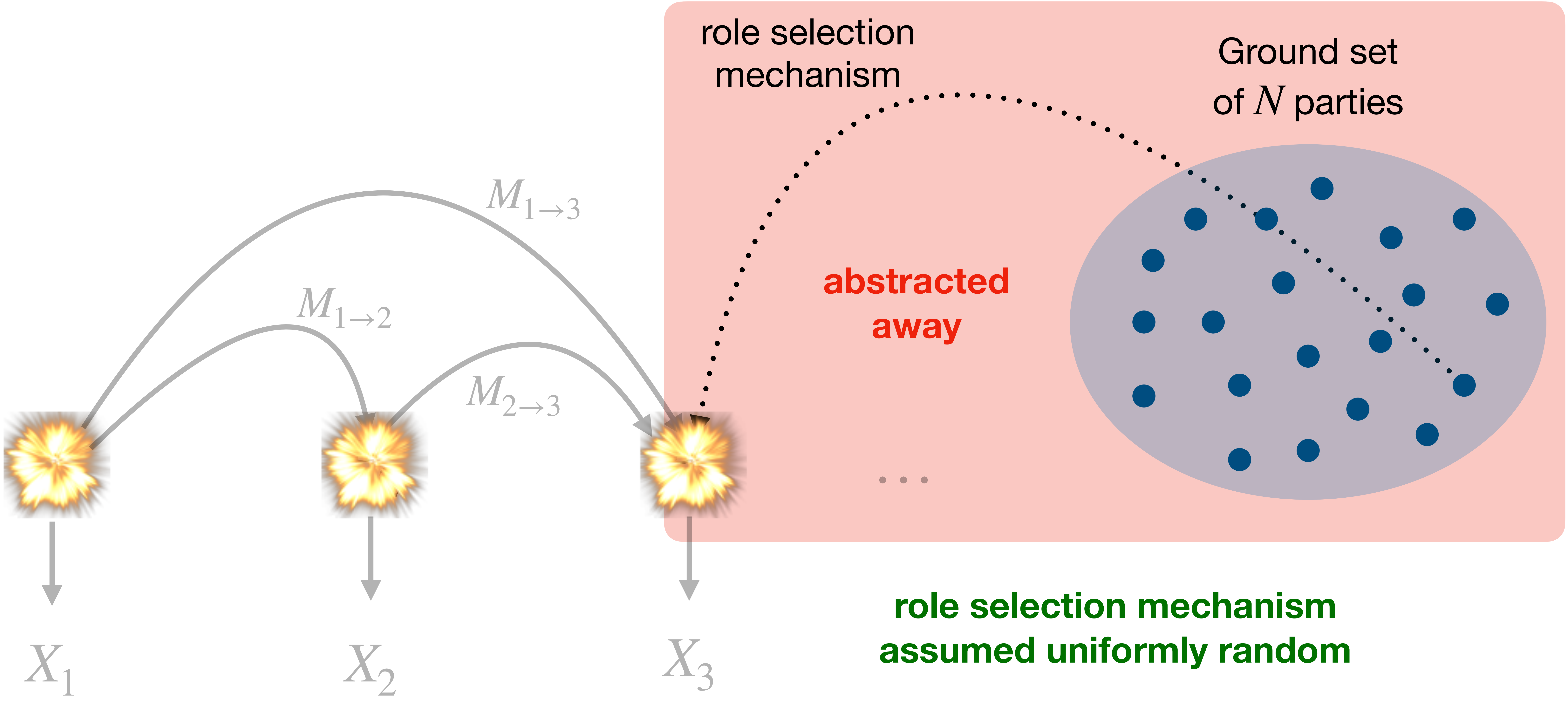
Craig Gentry[1], Shai Halevi[1], Hugo Krawczyk[1], Bernardo Magri[2], Jesper Buus Nielsen[*2], Tal Rabin[1], and Sophia Yakoubov[†3]

YOSO: You Only Speak Once

Secure MPC with Stateless Ephemeral Roles

Craig Gentry[1], Shai Halevi[1], Hugo Krawczyk[1], Bernardo Magri[2], Jesper Buus Nielsen[*2], Tal Rabin[1], and Sophia Yakoubov[†3]

n ephemeral roles, $n \ll N$



role selection mechanism assumed uniformly random

$\Longrightarrow$ **MPC with $t = (1/2 - \delta)N$ corruptions!**

YOSO *public* randomness extraction with worst-case corruptions

Replace i.i.d. random corruptions by **static chosen corruptions**

R_1 R_2 R_3 R_4

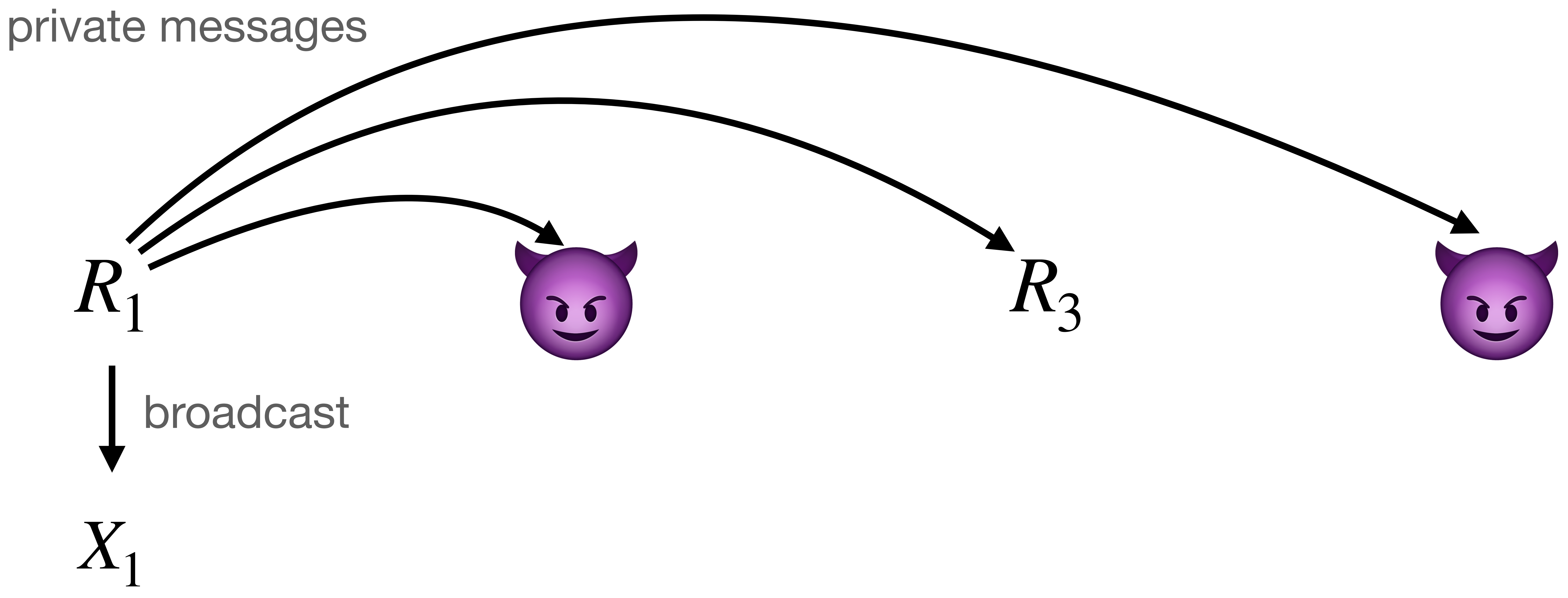
YOSO *public* randomness extraction with worst-case corruptions

Replace i.i.d. random corruptions by **static chosen corruptions**

R_1 😈 R_3 😈

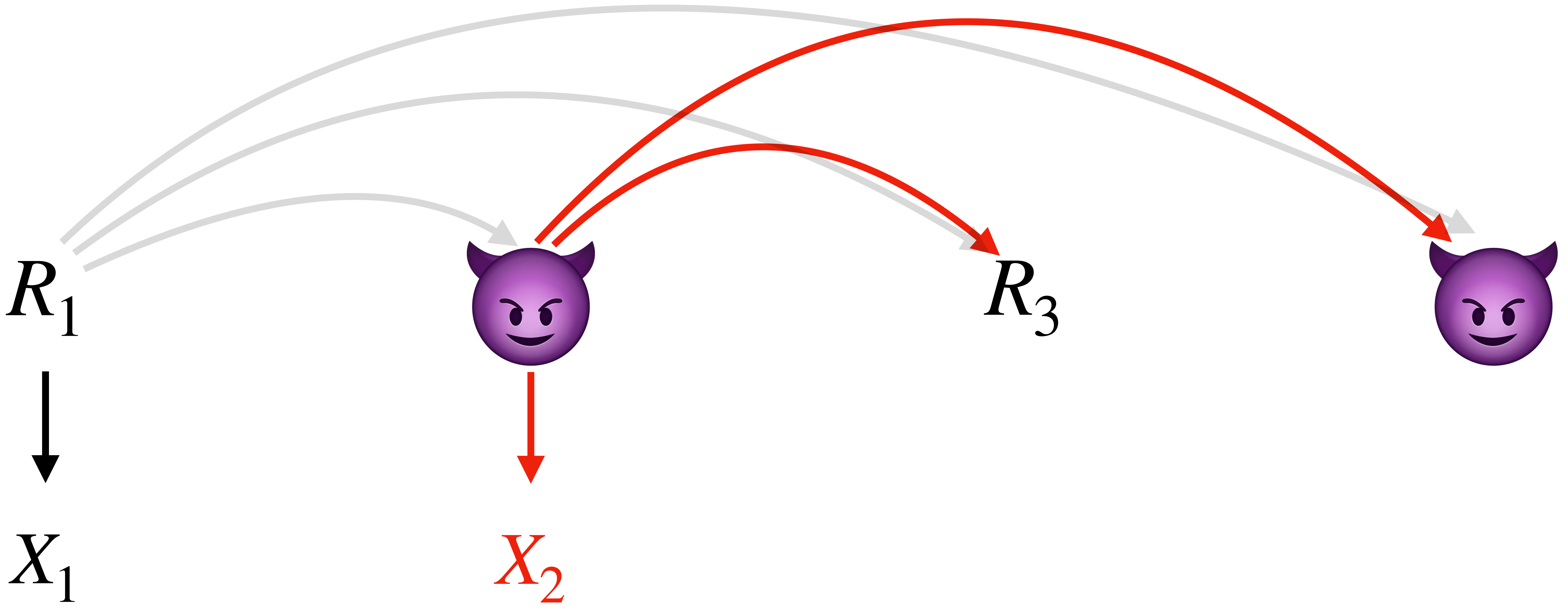
YOSO *public* randomness extraction with worst-case corruptions

Replace i.i.d. random corruptions by **static chosen corruptions**



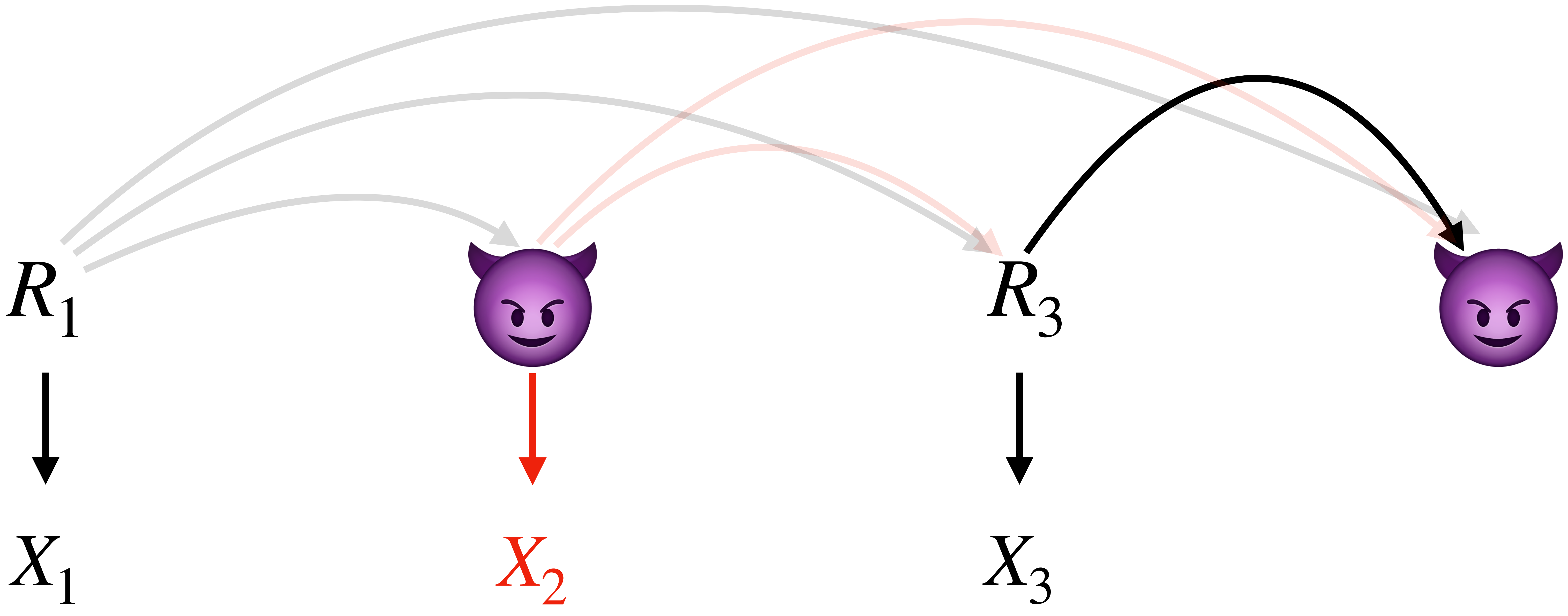
YOSO *public* randomness extraction with worst-case corruptions

Replace i.i.d. random corruptions by **static chosen corruptions**



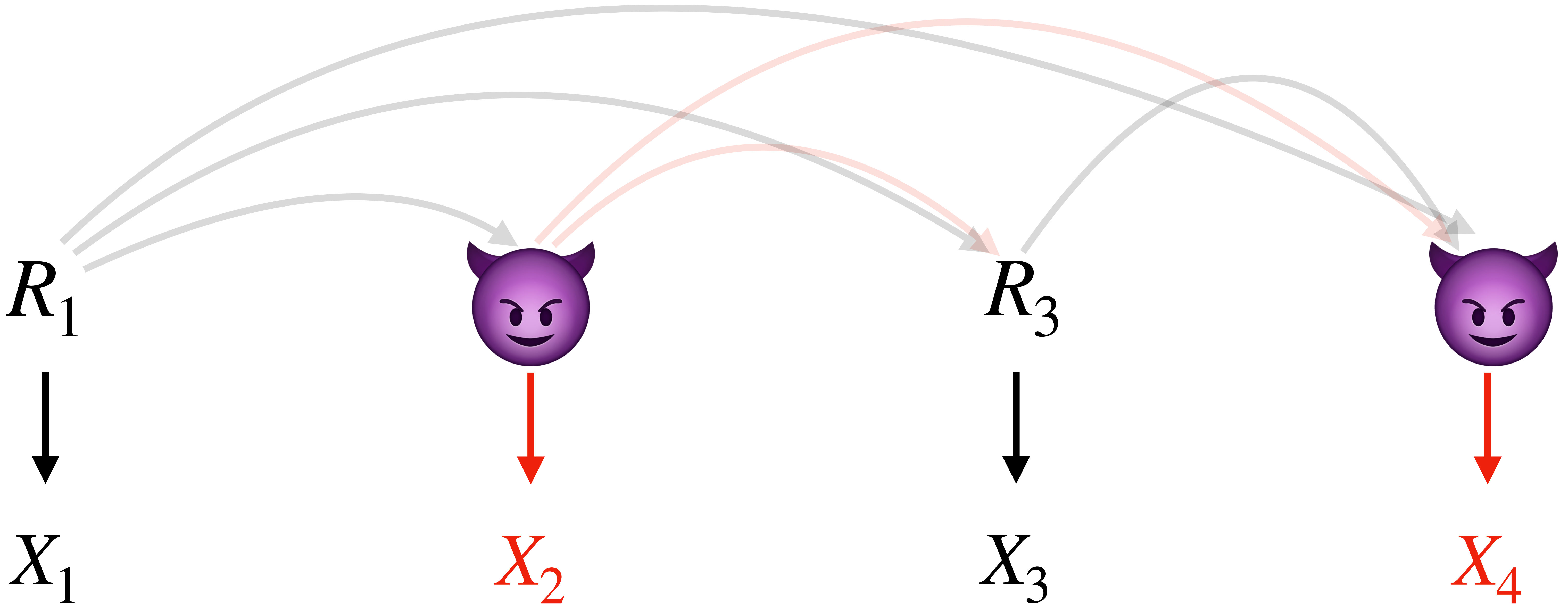
YOSO *public* randomness extraction with worst-case corruptions

Replace i.i.d. random corruptions by **static chosen corruptions**



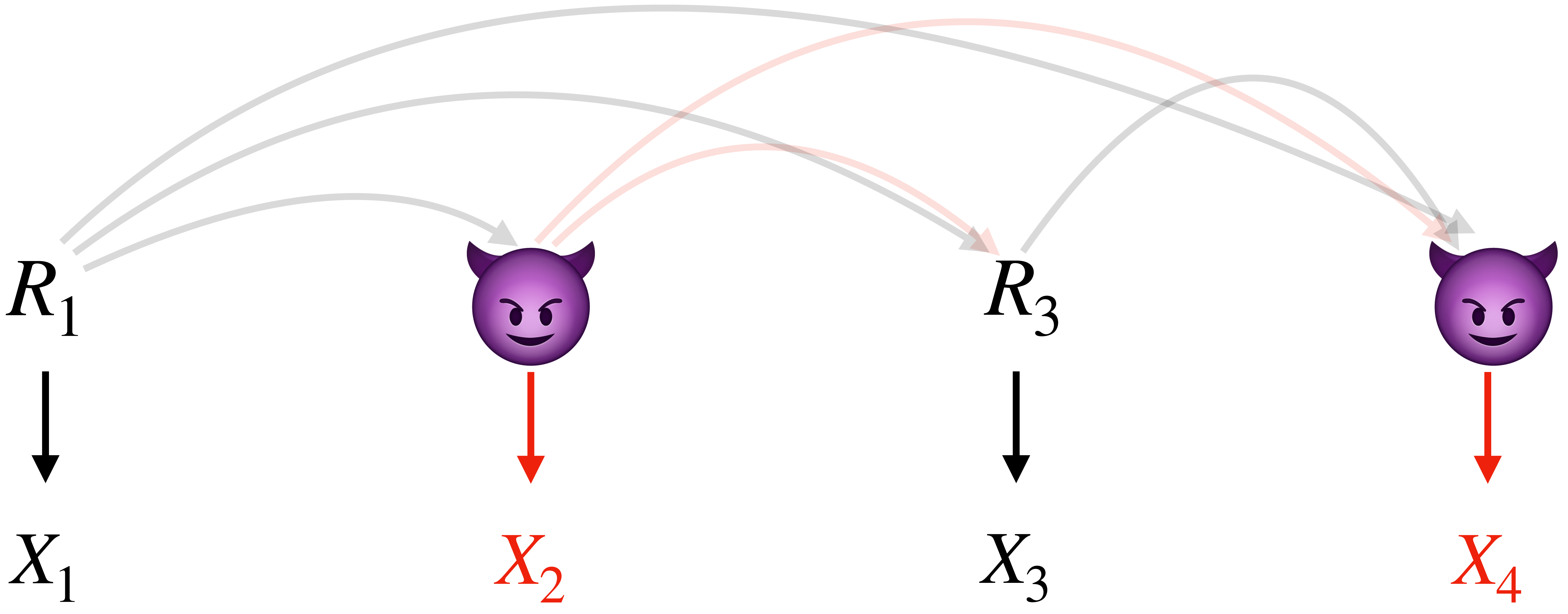
YOSO *public* randomness extraction with worst-case corruptions

Replace i.i.d. random corruptions by **static chosen corruptions**



YOSO *public* randomness extraction with worst-case corruptions

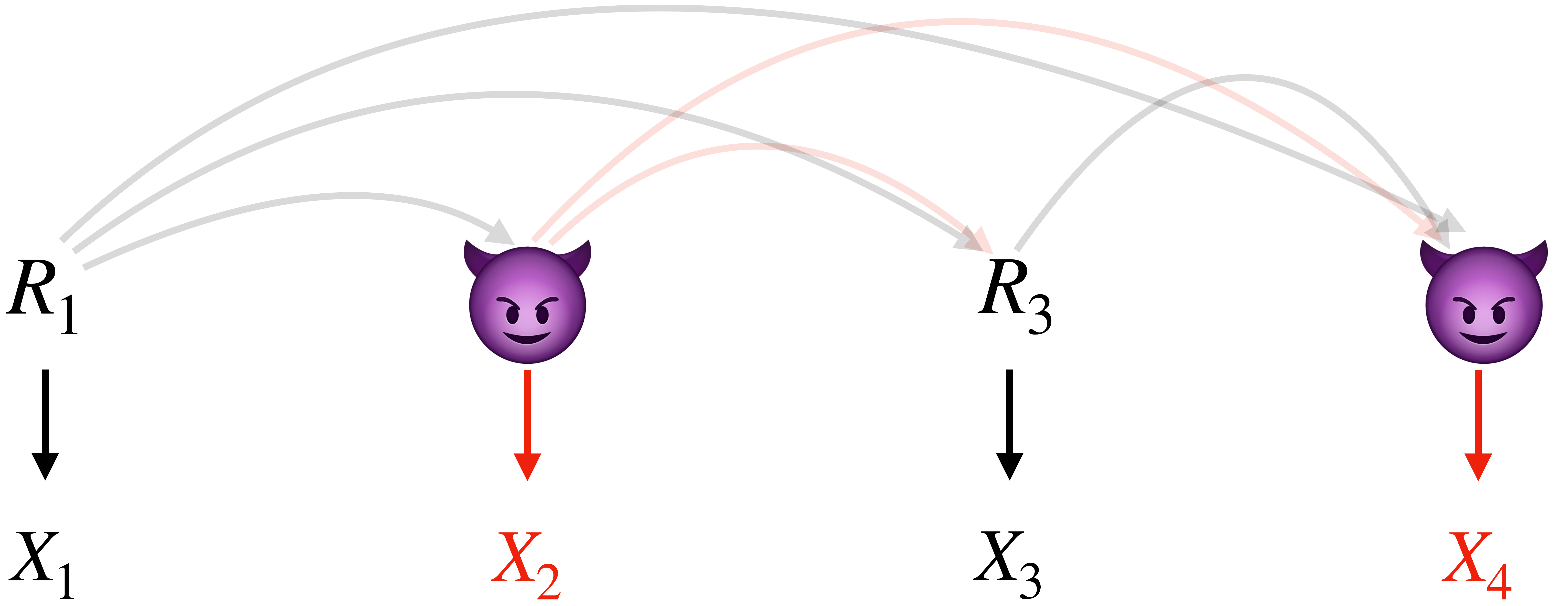
Replace i.i.d. random corruptions by **static chosen corruptions**



$$B = \mathrm{Ext}(X_1, X_2, X_3, X_4) \approx \mathrm{Unif}$$

YOSO *public* randomness extraction with worst-case corruptions

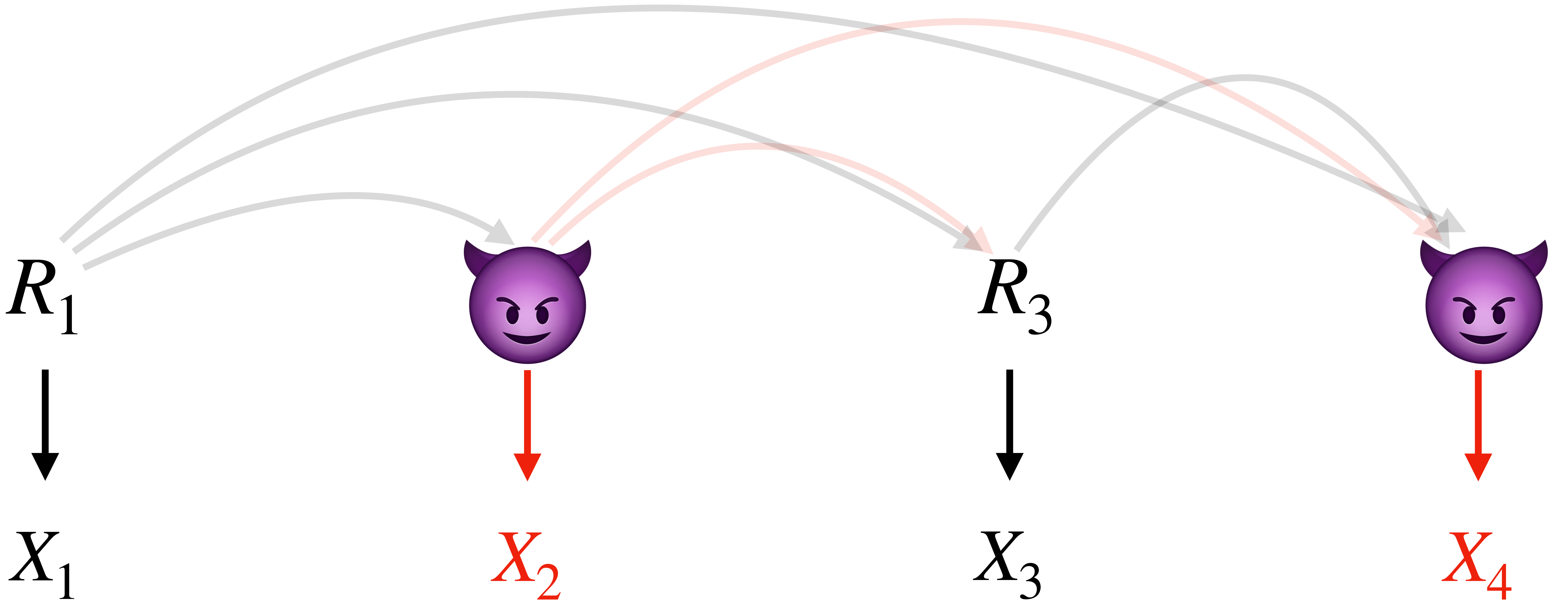
Replace i.i.d. random corruptions by **static chosen corruptions**



$$B = \mathrm{Ext}\underbrace{(X_1, X_2, X_3, X_4)}_{\text{only public values}} \approx \mathrm{Unif}$$

YOSO *public* randomness extraction with worst-case corruptions

Replace i.i.d. random corruptions by **static chosen corruptions**

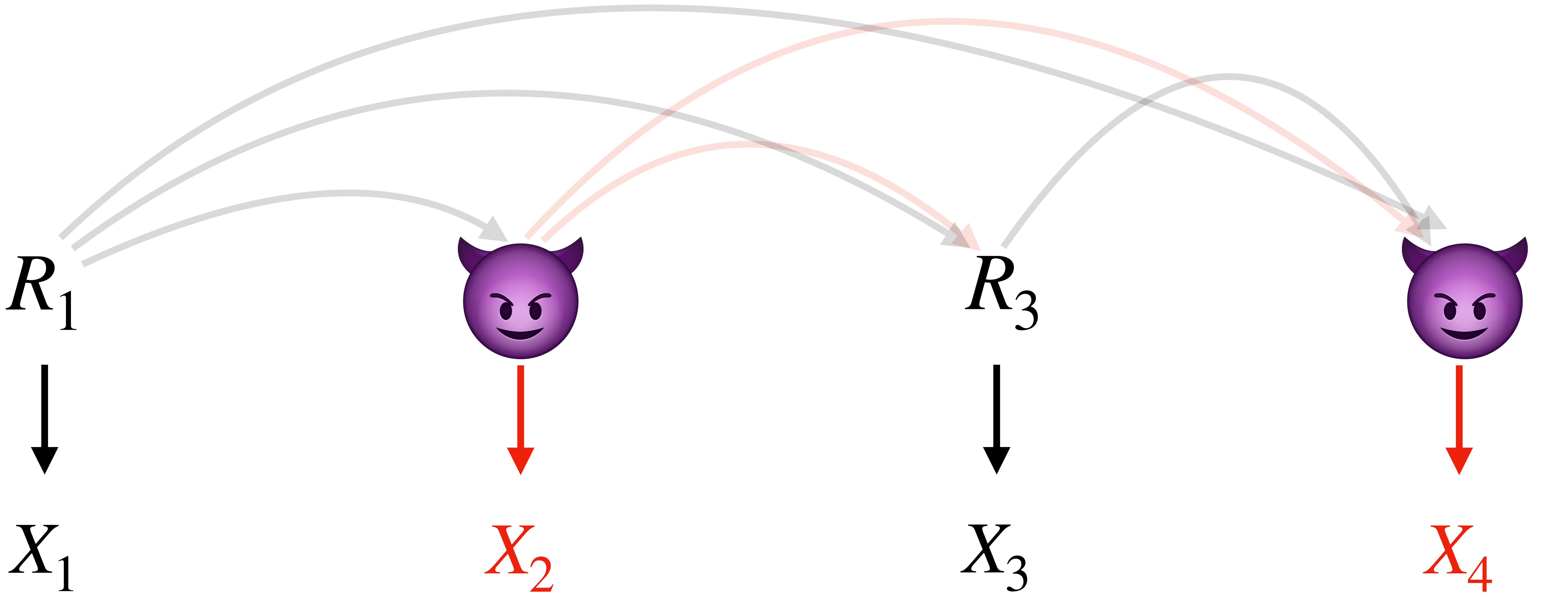


Why study worst-case corruptions?

$$B = \mathrm{Ext}\underbrace{(X_1, X_2, X_3, X_4)}_{\text{only public values}} \approx \mathrm{Unif}$$

YOSO *public* randomness extraction with worst-case corruptions

Replace i.i.d. random corruptions by **static chosen corruptions**



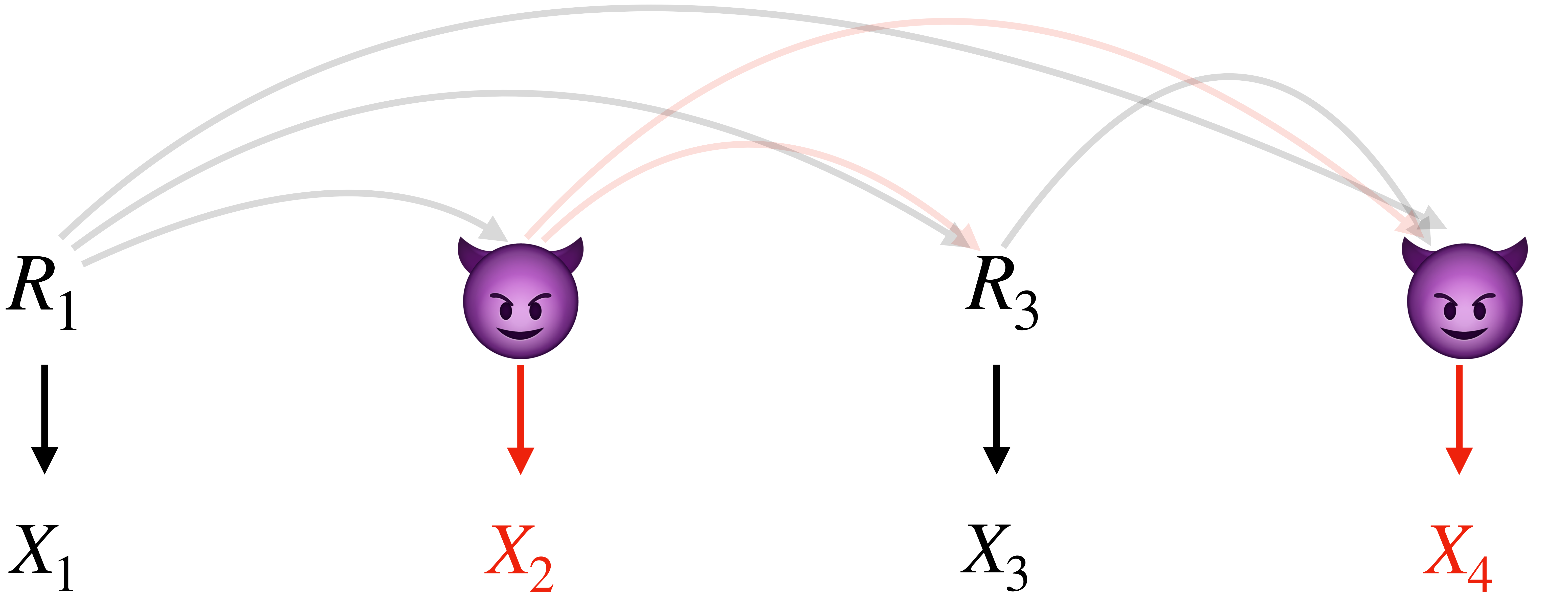
Why study worst-case corruptions?

- Role selection mechanism may be biased!

$$B = \mathrm{Ext}(\underbrace{X_1, X_2, X_3, X_4}_{\text{only public values}}) \approx \mathrm{Unif}$$

YOSO *public* randomness extraction with worst-case corruptions

Replace i.i.d. random corruptions by **static chosen corruptions**



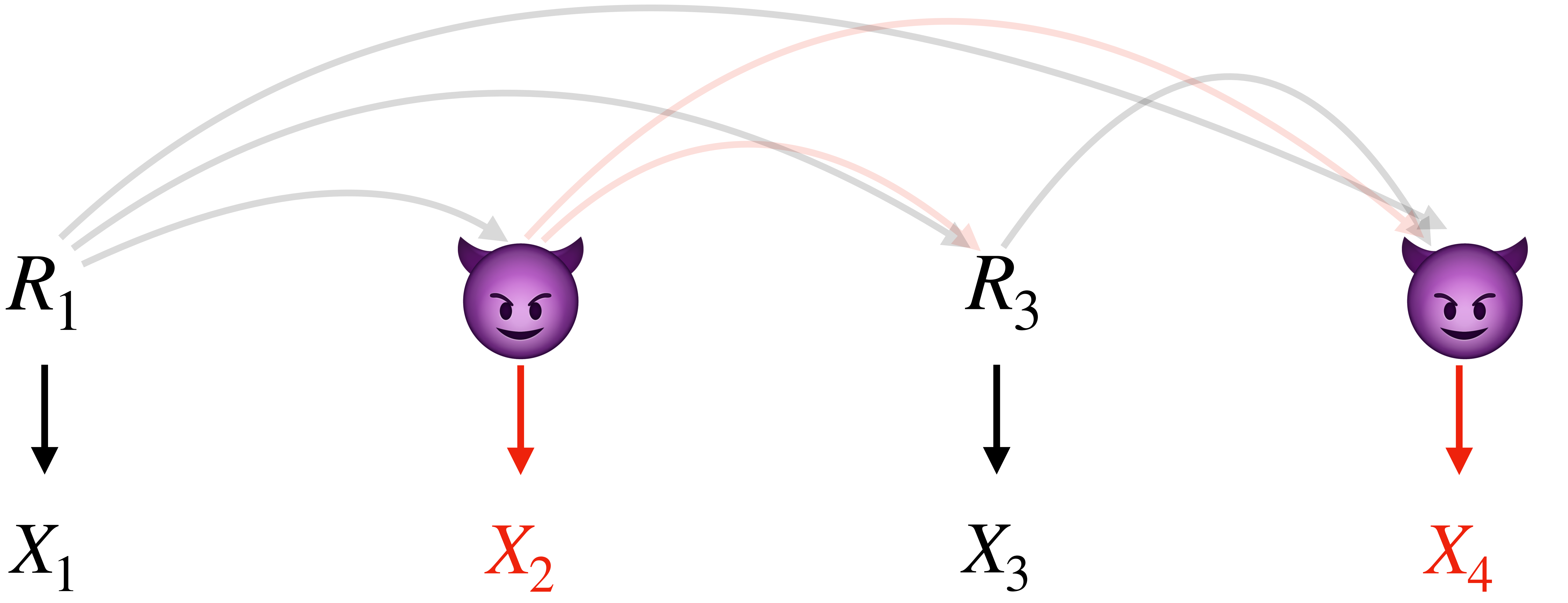
Why study worst-case corruptions?

- Role selection mechanism may be biased!
- Go beyond round-based MPC techniques

$$B = \mathrm{Ext}(\underbrace{X_1, X_2, X_3, X_4}_{\text{only public values}}) \approx \mathrm{Unif}$$

YOSO *public* randomness extraction with worst-case corruptions

Replace i.i.d. random corruptions by **static chosen corruptions**



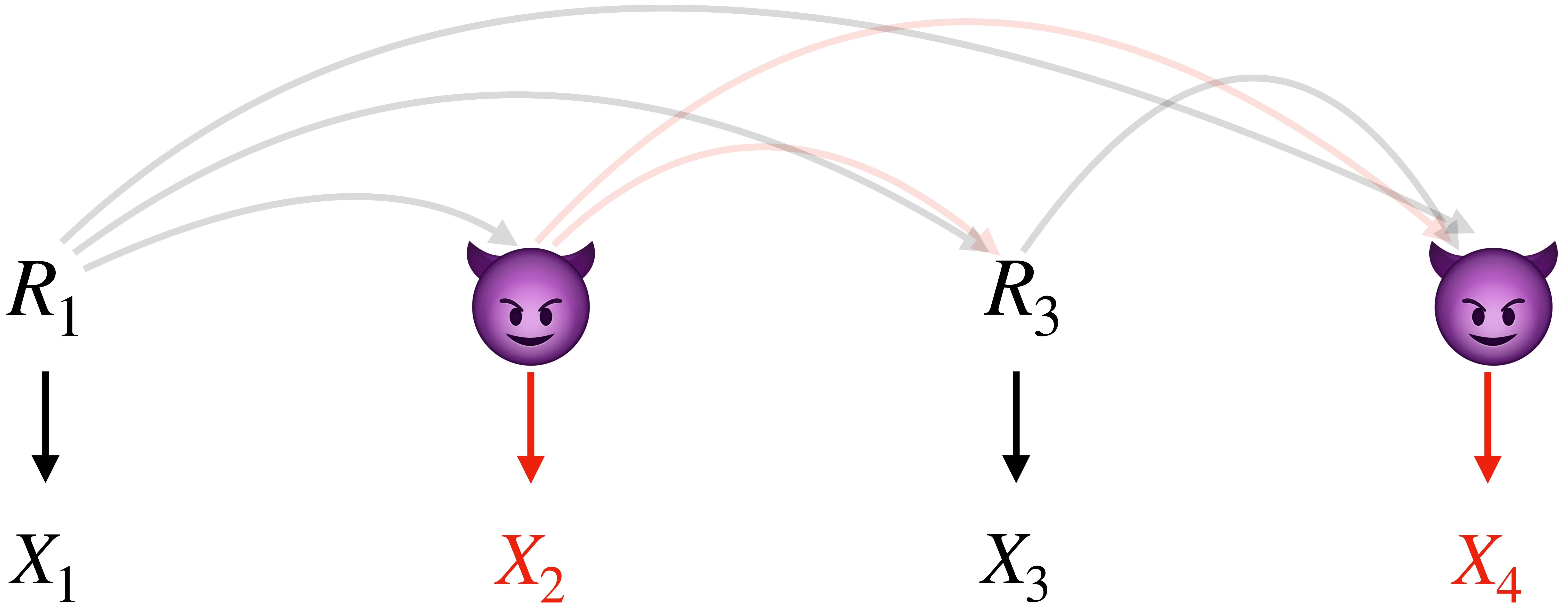
Why study worst-case corruptions?

- Role selection mechanism may be biased!
- Go beyond round-based MPC techniques
- Clean model

$$B = \mathrm{Ext}(\underbrace{X_1, X_2, X_3, X_4}_{\text{only public values}}) \approx \mathrm{Unif}$$

YOSO *public* randomness extraction with worst-case corruptions

Replace i.i.d. random corruptions by **static chosen corruptions**

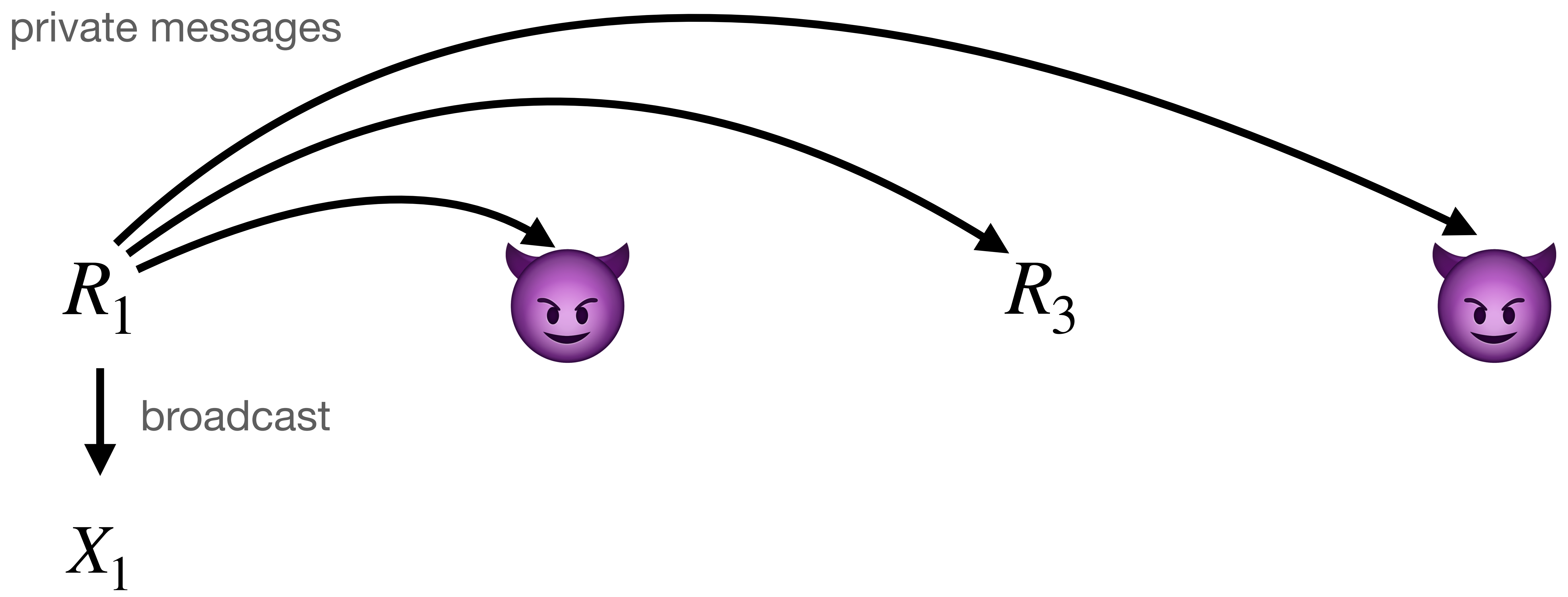


Why study worst-case corruptions?

- Role selection mechanism may be biased!
- Go beyond round-based MPC techniques
- Clean model
- Relationship to other randomness extraction settings

$$B = \mathrm{Ext}\underbrace{(X_1, X_2, X_3, X_4)}_{\text{only public values}} \approx \mathrm{Unif}$$

How are "messages to the future" implemented?

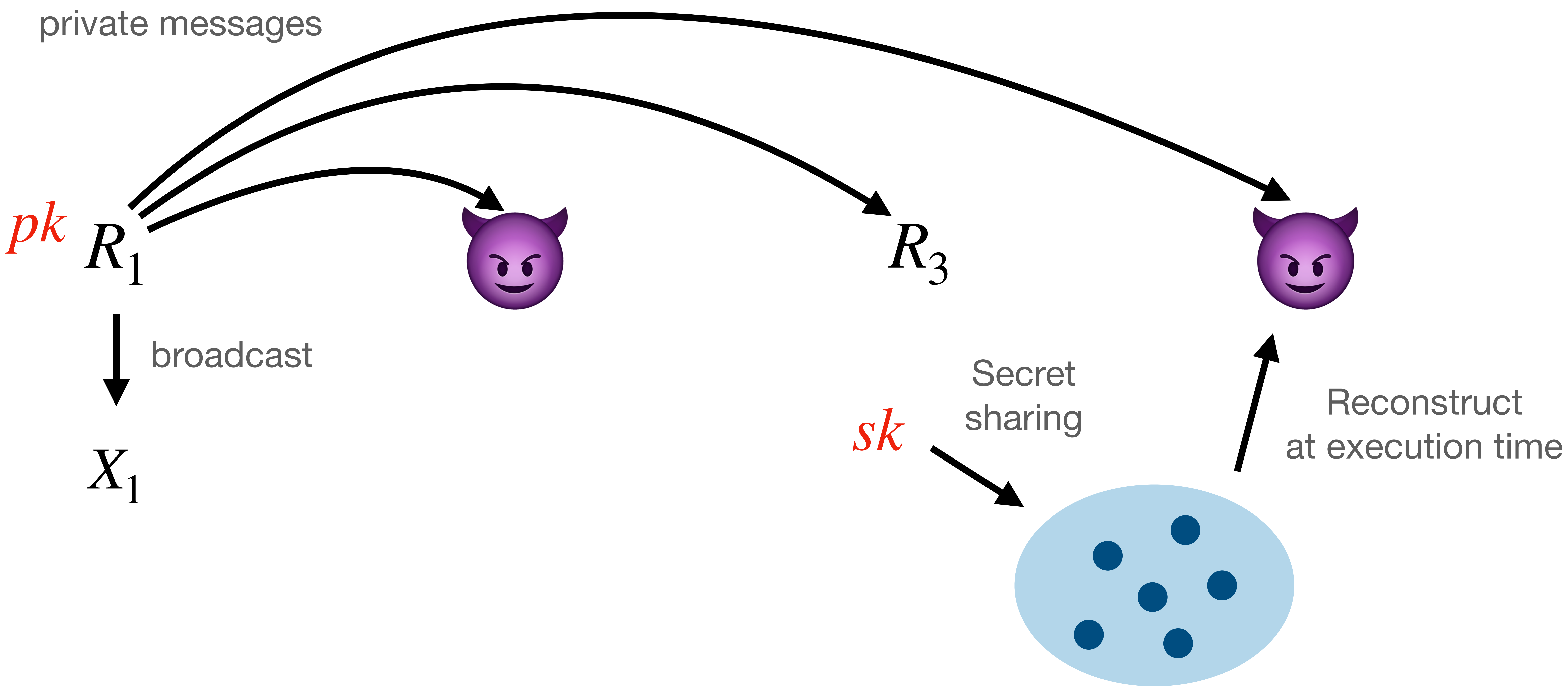


Simple models inspired by concrete implementations of such a mechanism.

In this talk: Adversary learns incoming messages to corrupted role *only when role is executed*

[Campanelli-David-Khoshakhlagh-Kristensen-Nielsen '21]

How are “messages to the future” implemented?

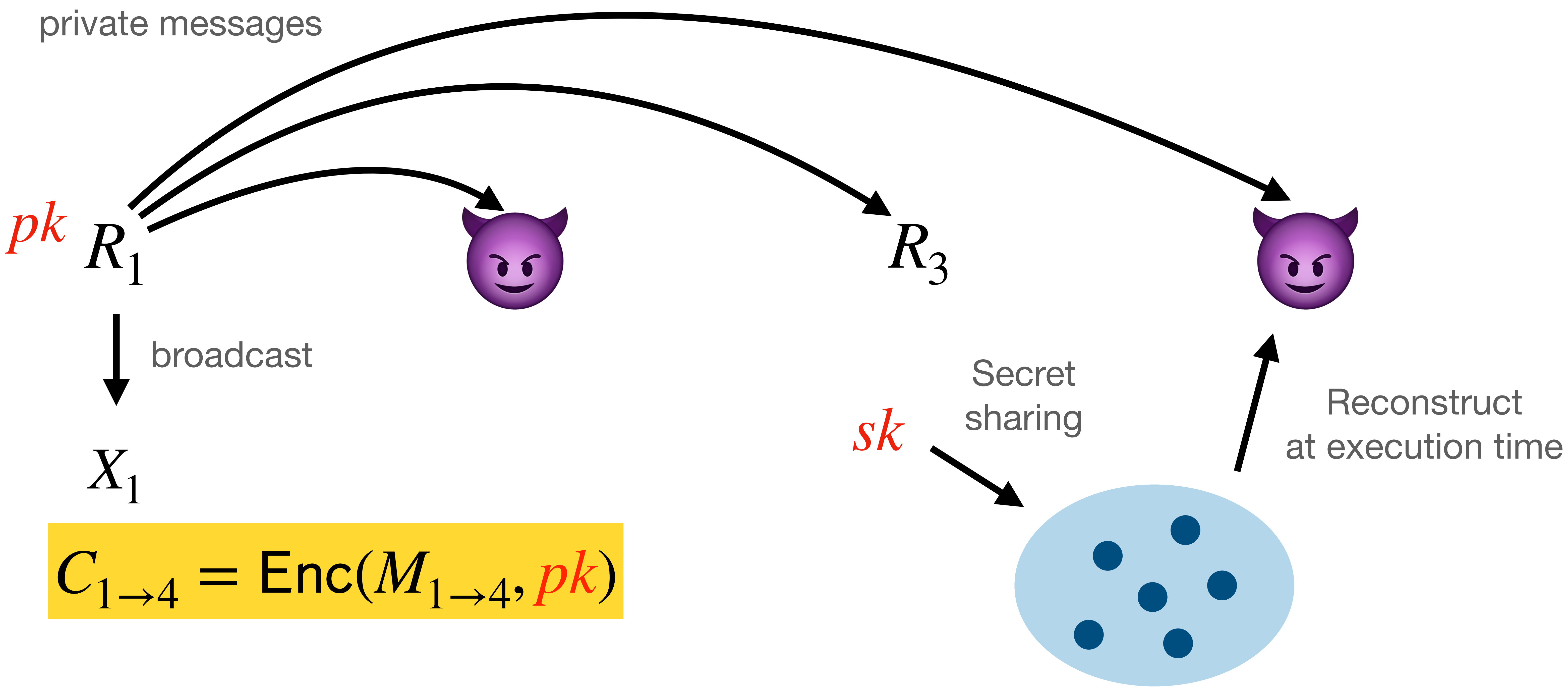


Simple models inspired by concrete implementations of such a mechanism.

In this talk: Adversary learns incoming messages to corrupted role *only when role is executed*

[Campanelli-David-Khoshakhlagh-Kristensen-Nielsen ’21]

How are “messages to the future” implemented?

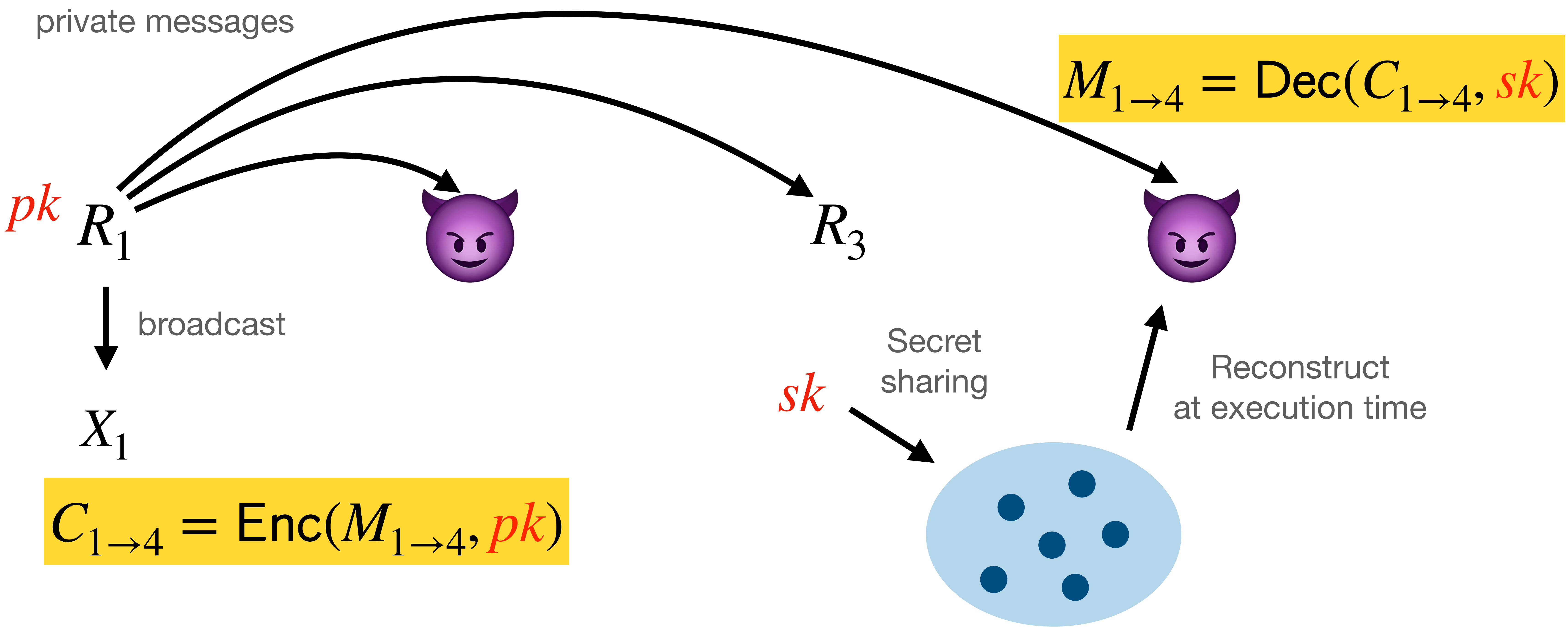


Simple models inspired by concrete implementations of such a mechanism.

In this talk: Adversary learns incoming messages to corrupted role *only when role is executed*

[Campanelli-David-Khoshakhlagh-Kristensen-Nielsen ’21]

How are “messages to the future” implemented?



Simple models inspired by concrete implementations of such a mechanism.

In this talk: Adversary learns incoming messages to corrupted role *only when role is executed*

[Campanelli-David-Khoshakhlagh-Kristensen-Nielsen ’21]

Our central question

What is the maximum corruption rate that allows for low-bias randomness extraction?

A naive approach to YOSO protocols

Starting point: Round-based n-party r-round protocol secure against $t = \delta n$ corruptions.

A naive approach to YOSO protocols

Starting point: Round-based n-party r-round protocol secure against $t = \delta n$ corruptions.

Emulate rounds in YOSO:

$$P_1^{(1)} \; \dots \; P_n^{(1)} \qquad P_1^{(2)} \; \dots \; P_n^{(2)} \qquad \dots \qquad P_1^{(r)} \; \dots \; P_n^{(r)}$$

A naive approach to YOSO protocols

Starting point: Round-based n-party r-round protocol secure against $t = \delta n$ corruptions.

Emulate rounds in YOSO:

$$P_1^{(1)} \;\ldots\; P_n^{(1)} \qquad P_1^{(2)} \;\ldots\; P_n^{(2)} \qquad \ldots \qquad P_1^{(r)} \;\ldots\; P_n^{(r)}$$

emulate round 1

A naive approach to YOSO protocols

Starting point: Round-based n-party r-round protocol secure against $t = \delta n$ corruptions.

Emulate rounds in YOSO:

$P_i^{(j)}$ sends secret state to $P_i^{(j+1)}$

$$P_1^{(1)} \ \dots \ P_n^{(1)} \qquad P_1^{(2)} \ \dots \ P_n^{(2)} \qquad \dots \qquad P_1^{(r)} \ \dots \ P_n^{(r)}$$

emulate round 1

A naive approach to YOSO protocols

Starting point: Round-based n-party r-round protocol secure against $t = \delta n$ corruptions.

Emulate rounds in YOSO:

$P_i^{(j)}$ sends secret state to $P_i^{(j+1)}$

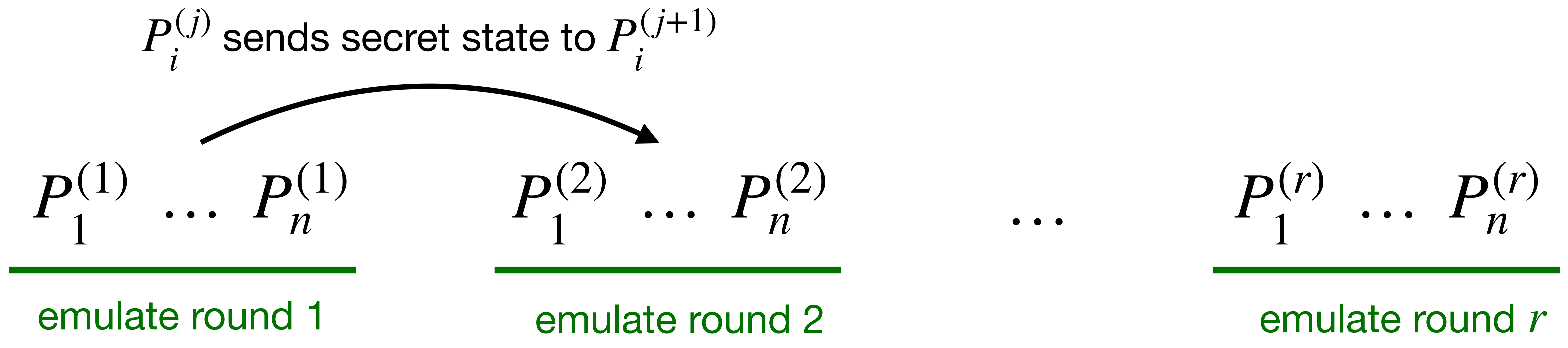
$P_1^{(1)} \; \dots \; P_n^{(1)}$ $\qquad$ $P_1^{(2)} \; \dots \; P_n^{(2)}$ $\qquad \dots \qquad$ $P_1^{(r)} \; \dots \; P_n^{(r)}$

emulate round 1 $\qquad$ emulate round 2 $\qquad$ emulate round r

A naive approach to YOSO protocols

Starting point: Round-based n-party r-round protocol secure against $t = \delta n$ corruptions.

Emulate rounds in YOSO:



Tolerated corruption rate decreased from δ to δ/r

A naive approach to YOSO protocols

Starting point: Round-based n-party r-round protocol secure against $t = \delta n$ corruptions.

Emulate rounds in YOSO:

$P_i^{(j)}$ sends secret state to $P_i^{(j+1)}$

$P_1^{(1)} \ \ldots \ P_n^{(1)}$ $P_1^{(2)} \ \ldots \ P_n^{(2)}$ $\ldots$ $P_1^{(r)} \ \ldots \ P_n^{(r)}$

emulate round 1   emulate round 2   emulate round r

Tolerated corruption rate decreased from δ to δ / r

3 rounds, $\delta \approx 1/3$ corruption rate $\Longrightarrow$ YOSO protocol secure against $\approx 1/9$ corruption rate

Our results

Feasibility

Impossibility

Our results

Feasibility

Zero-error randomness extraction against t corruptions
with $n = 5t$ roles
(or $n = 6t + 1$ roles against stronger adversary)

Impossibility

Our results

Feasibility

Zero-error randomness extraction against t corruptions
with $n = 5t$ roles
(or $n = 6t + 1$ roles against stronger adversary)

Impossibility

Randomness extraction with bias < 0.01
against t corruptions requires $n \geq 4t + 1$ roles

Protocol

There is a zero-error randomness extraction protocol secure against t chosen corruptions in the with $n = 5t + 2$ roles.

Protocol

There is a zero-error randomness extraction protocol secure against t chosen corruptions in the with $n = 5t + 2$ roles.

YOSOfied version of Maurer's "Secure MPC made simple"

Protocol

There is a zero-error randomness extraction protocol secure against t chosen corruptions in the with $n = 5t + 2$ roles.

YOSOfied version of Maurer's "Secure MPC made simple"

R_1 R_2 $\cdots$ R_{3t+1}

samplers

R'_1 R'_2 $\cdots$ R'_{2t+1}

publishers

Protocol

There is a zero-error randomness extraction protocol secure against t chosen corruptions in the with $n = 5t + 2$ roles.

YOSOfied version of Maurer's "Secure MPC made simple"

$R_1 \quad R_2 \quad \cdots \quad R_{3t+1}$

samplers

$R'_1 \quad R'_2 \quad \cdots \quad R'_{2t+1}$

publishers

High-level idea:

Protocol

There is a zero-error randomness extraction protocol secure against t chosen corruptions in the with $n = 5t + 2$ roles.

YOSOfied version of Maurer's "Secure MPC made simple"

R_1 R_2 $\cdots$ R_{3t+1}

samplers

R'_1 R'_2 $\cdots$ R'_{2t+1}

publishers

High-level idea:

1. Several subsets of samplers commit to values and send them to publishers;

Protocol

There is a zero-error randomness extraction protocol secure against t chosen corruptions in the with $n = 5t + 2$ roles.

YOSOfied version of Maurer's "Secure MPC made simple"

$$R_1 \quad R_2 \quad \cdots \quad R_{3t+1} \qquad\qquad R'_1 \quad R'_2 \quad \cdots \quad R'_{2t+1}$$

samplers publishers

High-level idea:

1. Several subsets of samplers commit to values and send them to publishers;
2. Publishers broadcast whatever they receive;

Protocol

There is a zero-error randomness extraction protocol secure against t chosen corruptions in the with $n = 5t + 2$ roles.

YOSOfied version of Maurer's "Secure MPC made simple"

$R_1 \quad R_2 \quad \cdots \quad R_{3t+1}$

samplers

$R'_1 \quad R'_2 \quad \cdots \quad R'_{2t+1}$

publishers

High-level idea:

1. Several subsets of samplers commit to values and send them to publishers;
2. Publishers broadcast whatever they receive;
3. Extract random bit by taking majorities and XOR.

Protocol

$S = \{i_1 < i_2 < \cdots < i_{2t+1}\} \subseteq [3t+1]$

publishers

R_{i_1} R_{i_2} $\cdots$ R_{i_j} $\cdots$ $R_{i_{2t+1}}$ R'_1 $\cdots$ R'_{2t+1}

samplers

Protocol

$S = \{i_1 < i_2 < \cdots < i_{2t+1}\} \subseteq [3t+1]$

publishers

$x_1 \leftarrow \{0,1\}$

R_{i_1} R_{i_2} $\cdots$ R_{i_j} $\cdots$ $R_{i_{2t+1}}$ R'_1 $\cdots$ R'_{2t+1}

samplers

Protocol

$S = \{i_1 < i_2 < \cdots < i_{2t+1}\} \subseteq [3t+1]$

x_1

publishers

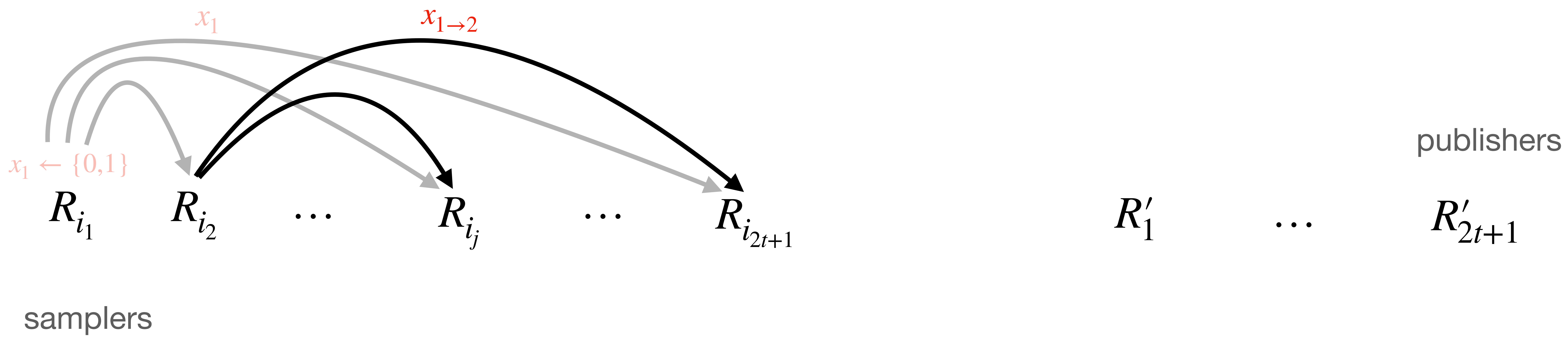
$x_1 \leftarrow \{0,1\}$

R_{i_1} R_{i_2} $\ldots$ R_{i_j} $\ldots$ $R_{i_{2t+1}}$ R'_1 $\ldots$ R'_{2t+1}

samplers

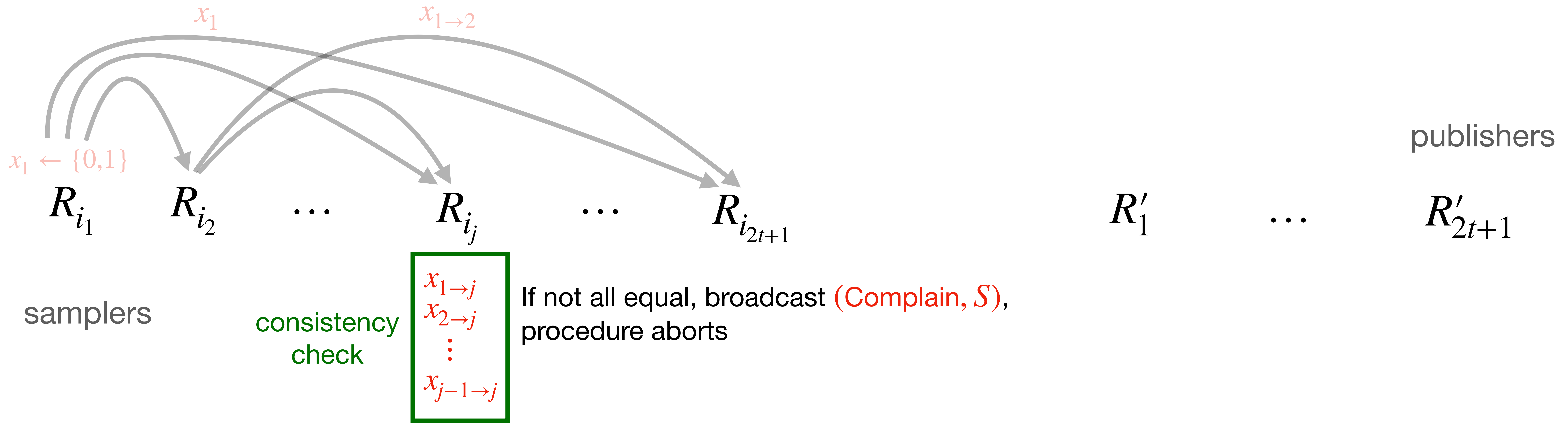
Protocol

$$S = \{i_1 < i_2 < \cdots < i_{2t+1}\} \subseteq [3t+1]$$



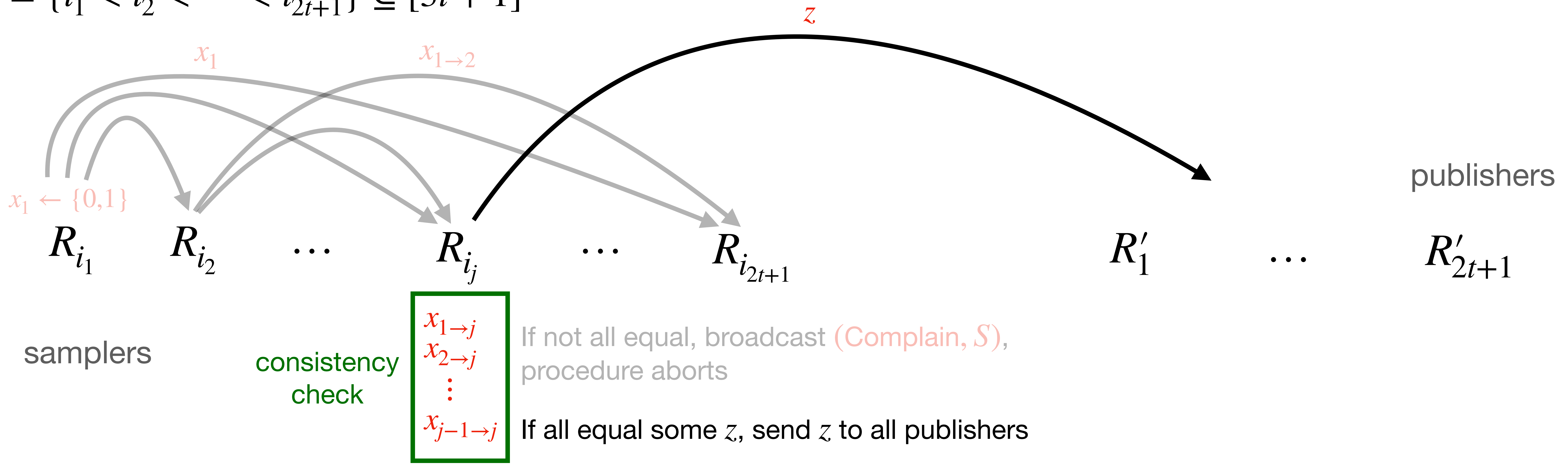
Protocol

$S = \{i_1 < i_2 < \cdots < i_{2t+1}\} \subseteq [3t+1]$



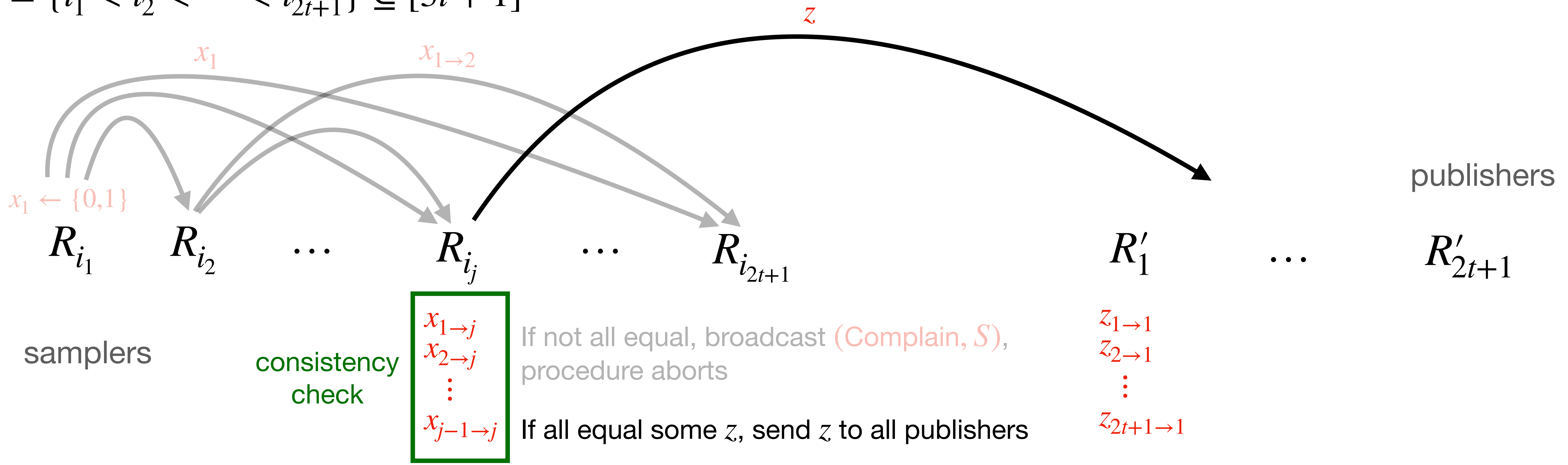
Protocol

$$S = \{i_1 < i_2 < \cdots < i_{2t+1}\} \subseteq [3t+1]$$

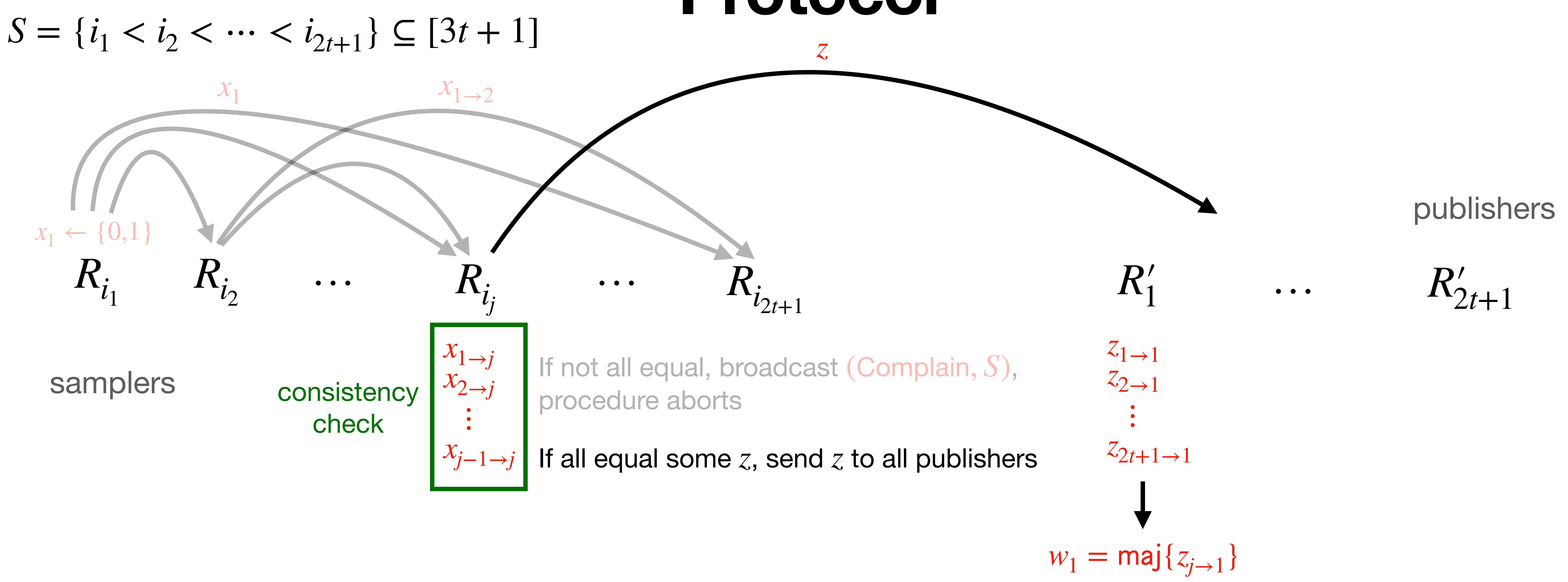


Protocol

$$S = \{i_1 < i_2 < \cdots < i_{2t+1}\} \subseteq [3t+1]$$



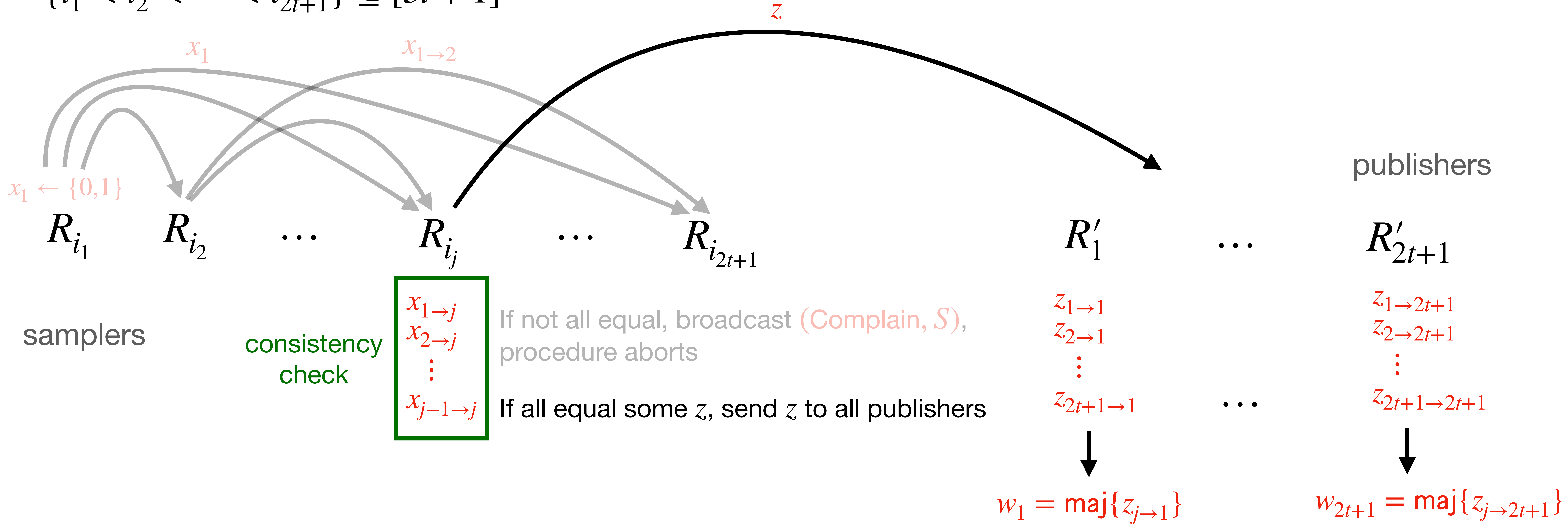
Protocol



$S = \{i_1 < i_2 < \cdots < i_{2t+1}\} \subseteq [3t+1]$
z
x_1
$x_{1\to 2}$
$x_1 \leftarrow \{0,1\}$
publishers
R_{i_1} R_{i_2} $\cdots$ R_{i_j} $\cdots$ $R_{i_{2t+1}}$
R'_1 $\cdots$ R'_{2t+1}
samplers
consistency check
$x_{1\to j}$
$x_{2\to j}$
$\vdots$
$x_{j-1\to j}$
If not all equal, broadcast (Complain, S), procedure aborts
If all equal some z, send z to all publishers
$z_{1\to 1}$
$z_{2\to 1}$
$\vdots$
$z_{2t+1\to 1}$
$w_1 =$ maj$\{z_{j\to 1}\}$

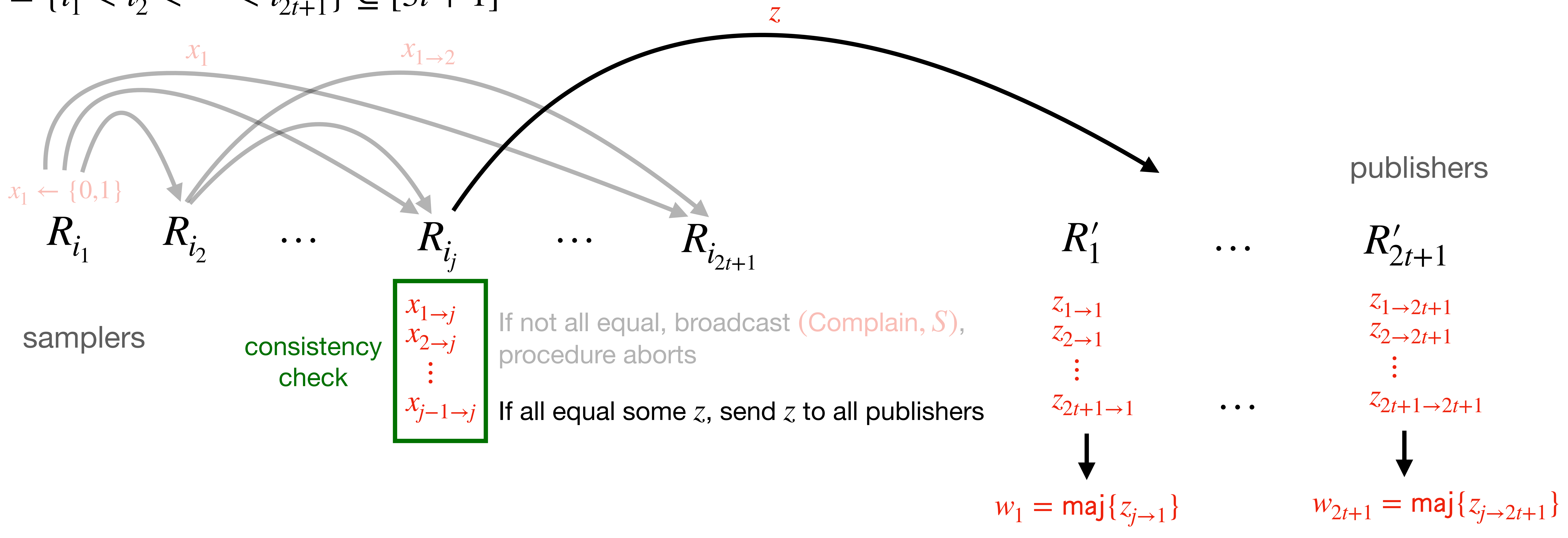
Protocol

$S = \{i_1 < i_2 < \cdots < i_{2t+1}\} \subseteq [3t+1]$



Protocol

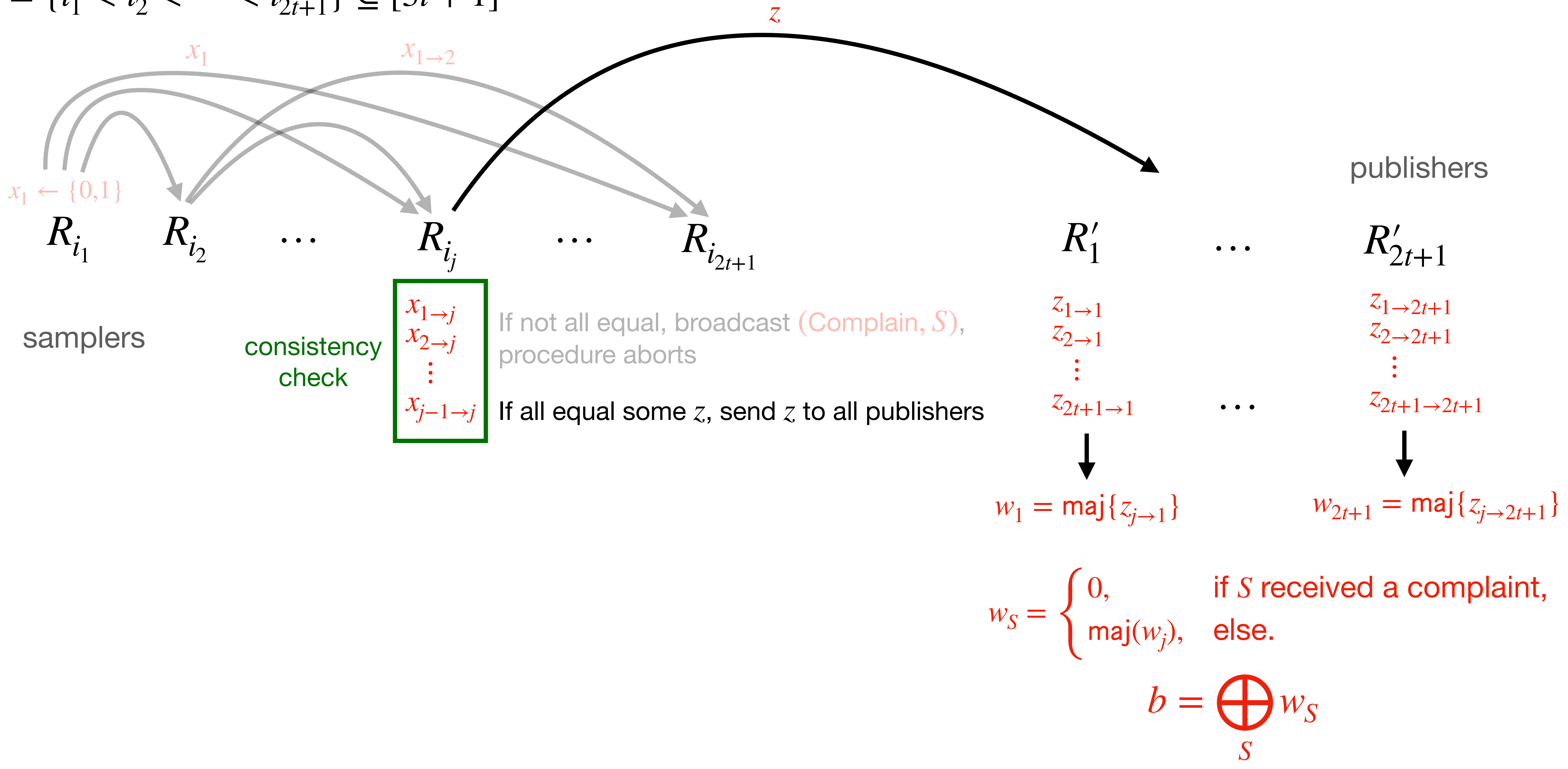
$S = \{i_1 < i_2 < \cdots < i_{2t+1}\} \subseteq [3t+1]$



$$w_S = \begin{cases} 0, & \text{if } S \text{ received a complaint,} \\ \text{maj}(w_j), & \text{else.} \end{cases}$$

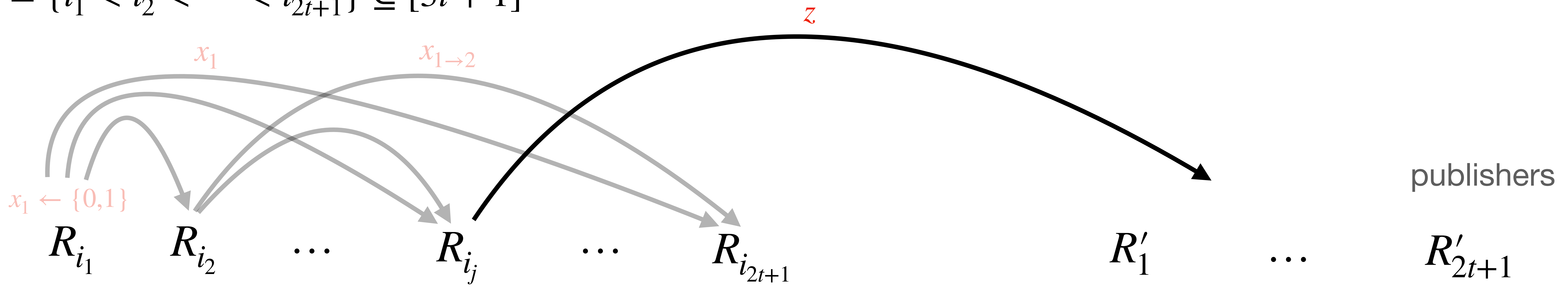
Protocol

$S = \{i_1 < i_2 < \cdots < i_{2t+1}\} \subseteq [3t+1]$



Protocol

$S = \{i_1 < i_2 < \cdots < i_{2t+1}\} \subseteq [3t+1]$



samplers

consistency check

$$\boxed{\begin{matrix} x_{1\to j} \\ x_{2\to j} \\ \vdots \\ x_{j-1\to j} \end{matrix}}$$

If not all equal, broadcast (Complain, S), procedure aborts

If all equal some z, send z to all publishers

$$\begin{matrix} z_{1\to 1} \\ z_{2\to 1} \\ \vdots \\ z_{2t+1\to 1} \end{matrix} \quad \cdots \quad \begin{matrix} z_{1\to 2t+1} \\ z_{2\to 2t+1} \\ \vdots \\ z_{2t+1\to 2t+1} \end{matrix}$$

$$w_1 = \text{maj}\{z_{j\to 1}\} \qquad w_{2t+1} = \text{maj}\{z_{j\to 2t+1}\}$$

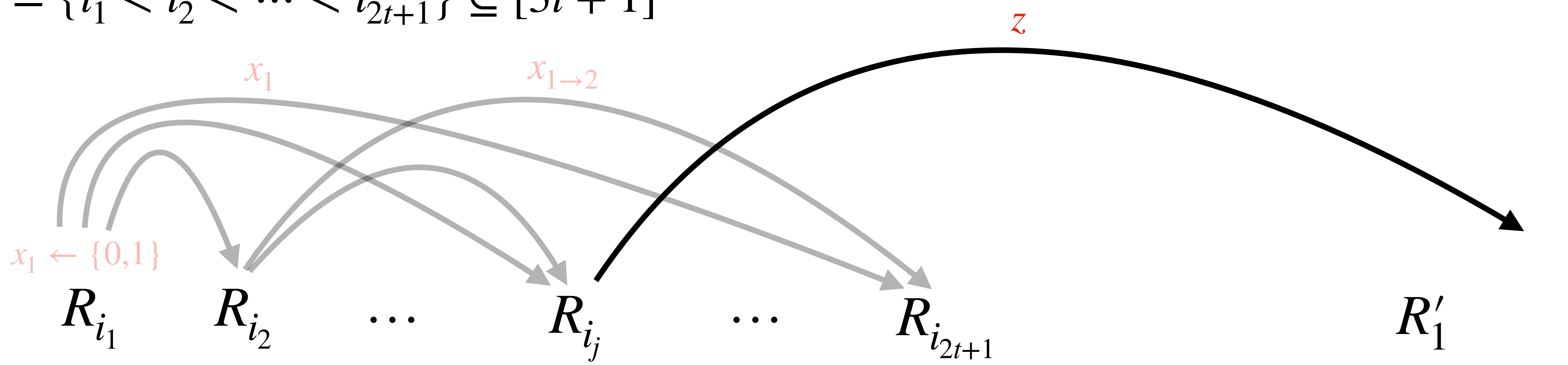
$$w_S = \begin{cases} 0, & \text{if } S \text{ received a complaint,} \\ \text{maj}(w_j), & \text{else.} \end{cases}$$

$$b = \bigoplus_S w_S$$

Key properties:

Protocol

$S = \{i_1 < i_2 < \cdots < i_{2t+1}\} \subseteq [3t+1]$



samplers

consistency check

$\boxed{\begin{matrix} x_{1\to j} \\ x_{2\to j} \\ \vdots \\ x_{j-1\to j} \end{matrix}}$

If not all equal, broadcast (Complain, S), procedure aborts

If all equal some z, send z to all publishers

$$\begin{matrix} z_{1\to 1} & & z_{1\to 2t+1} \\ z_{2\to 1} & & z_{2\to 2t+1} \\ \vdots & \cdots & \vdots \\ z_{2t+1\to 1} & \cdots & z_{2t+1\to 2t+1} \\ \downarrow & & \downarrow \\ w_1 = \mathrm{maj}\{z_{j\to 1}\} & & w_{2t+1} = \mathrm{maj}\{z_{j\to 2t+1}\} \end{matrix}$$

$$w_S = \begin{cases} 0, & \text{if } S \text{ received a complaint,} \\ \mathrm{maj}(w_j), & \text{else.} \end{cases}$$

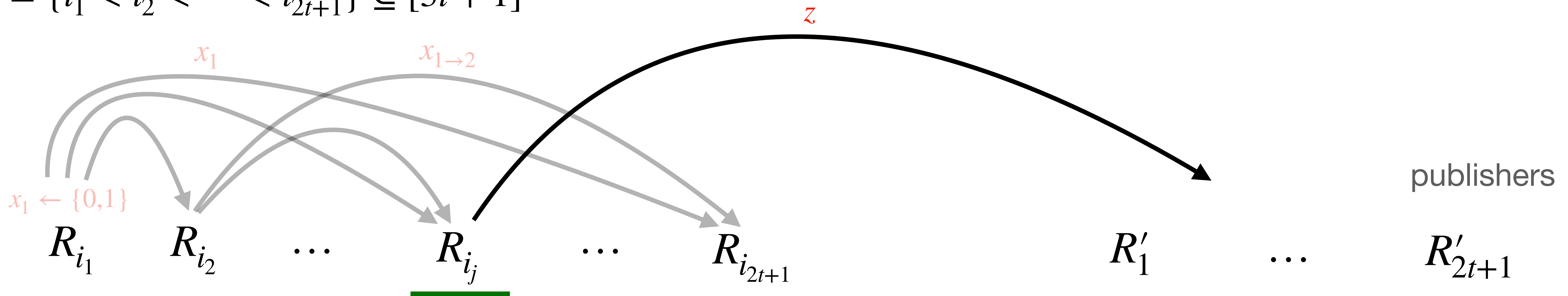
$$b = \bigoplus_S w_S$$

Key properties:

- Every set S has a strict honest majority;

Protocol

$S = \{i_1 < i_2 < \cdots < i_{2t+1}\} \subseteq [3t+1]$



samplers

consistency check

$\boxed{\begin{matrix} x_{1\to j} \\ x_{2\to j} \\ \vdots \\ x_{j-1\to j} \end{matrix}}$

If not all equal, broadcast (Complain, S), procedure aborts

If all equal some z, send z to all publishers

$z_{1\to 1}$, $z_{2\to 1}$, $\vdots$, $z_{2t+1\to 1}$ $\cdots$ $z_{1\to 2t+1}$, $z_{2\to 2t+1}$, $\vdots$, $z_{2t+1\to 2t+1}$

$w_1 = \text{maj}\{z_{j\to 1}\}$ $\qquad$ $w_{2t+1} = \text{maj}\{z_{j\to 2t+1}\}$

$$w_S = \begin{cases} 0, & \text{if } S \text{ received a complaint,} \\ \text{maj}(w_j), & \text{else.} \end{cases}$$

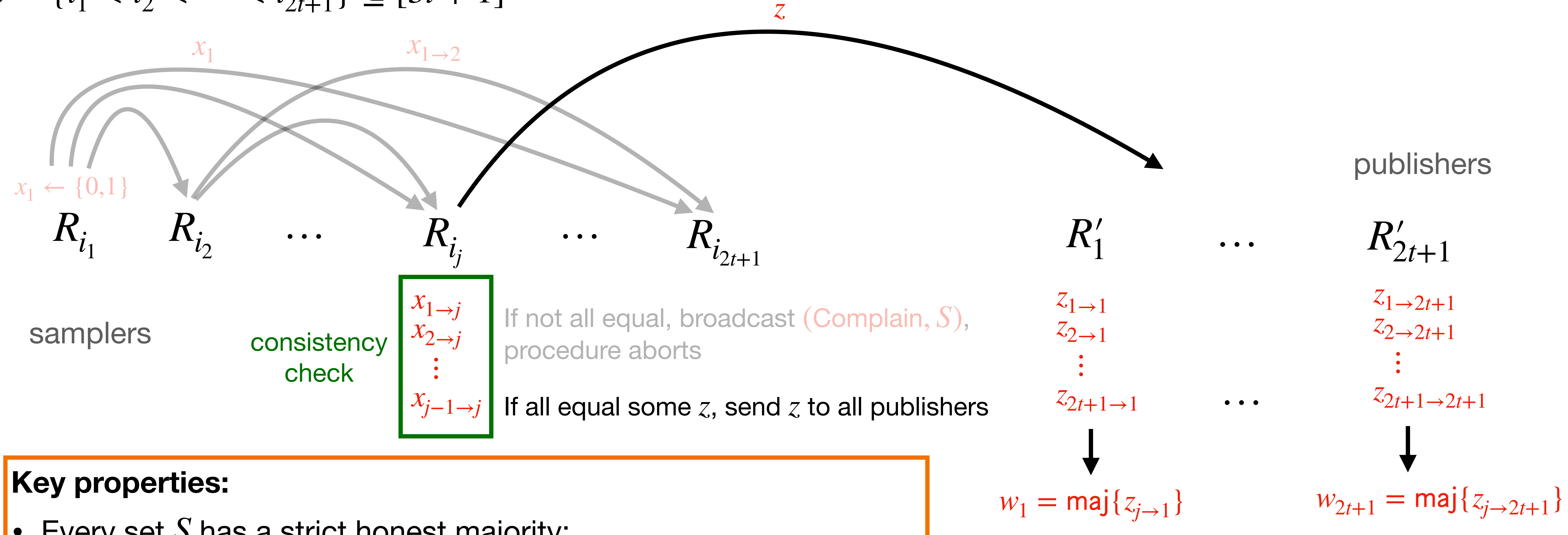
$$b = \bigoplus_S w_S$$

Key properties:

- Every set S has a strict honest majority;
- If S did not receive a complaint, then all honest roles in S agree on the same value;

Protocol

$S = \{i_1 < i_2 < \cdots < i_{2t+1}\} \subseteq [3t+1]$



Key properties:

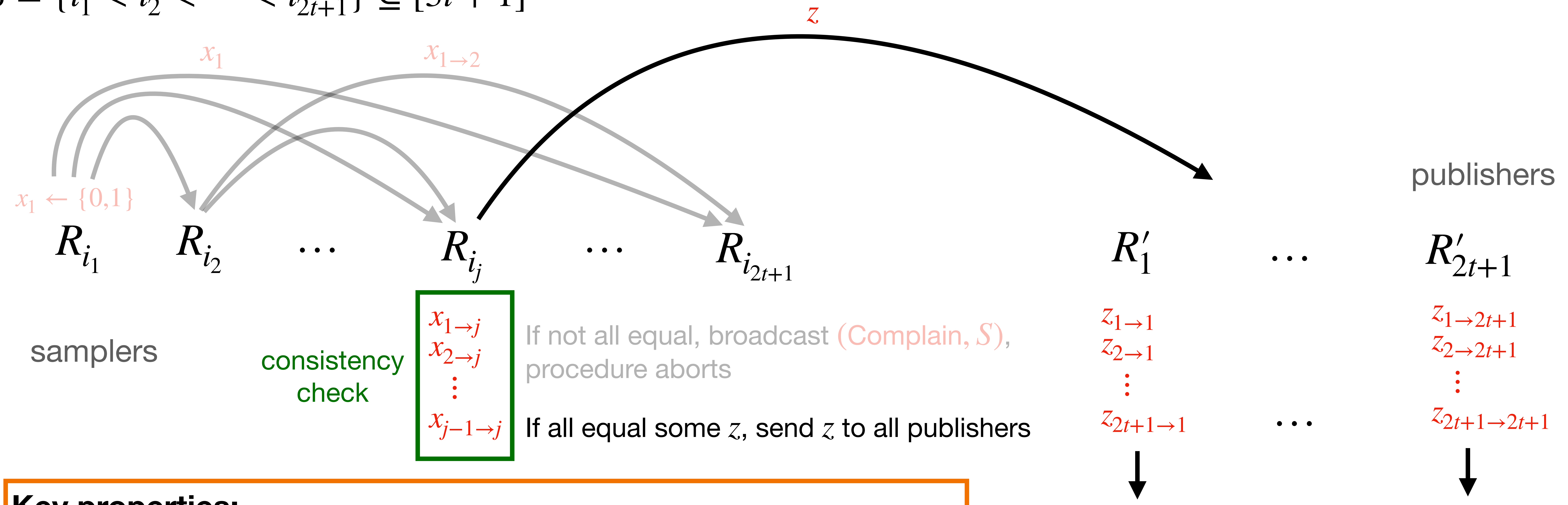
- Every set S has a strict honest majority;
- If S did not receive a complaint, then all honest roles in S agree on the same value;
- There is a set $S^\star$ such that all roles $(P_i)_{i\in S^\star}$ are honest.

$$w_S = \begin{cases} 0, & \text{if } S \text{ received a complaint,} \\ \mathrm{maj}(w_j), & \text{else.} \end{cases}$$

$$b = \bigoplus_S w_S$$

Protocol

$$S = \{i_1 < i_2 < \cdots < i_{2t+1}\} \subseteq [3t+1]$$



$w_1 = \text{maj}\{z_{j\to 1}\}$ $\quad$ $w_{2t+1} = \text{maj}\{z_{j\to 2t+1}\}$

Key properties:

- Every set S has a strict honest majority;
- If S did not receive a complaint, then all honest roles in S agree on the same value;
- There is a set $S^\star$ such that all roles $(P_i)_{i\in S^\star}$ are honest.

$\Longrightarrow$ $w_{S^\star}$ is uniform and independent of $(w_S)_{S\neq S^\star}$.

$$w_S = \begin{cases} 0, & \text{if } S \text{ received a complaint,} \\ \text{maj}(w_j), & \text{else.} \end{cases}$$

$$b = \bigoplus_S w_S$$

A simple improved protocol for one corruption

samplers

publishers

R_1 R_2 R'_1 R'_2 R'_3

A simple improved protocol for one corruption

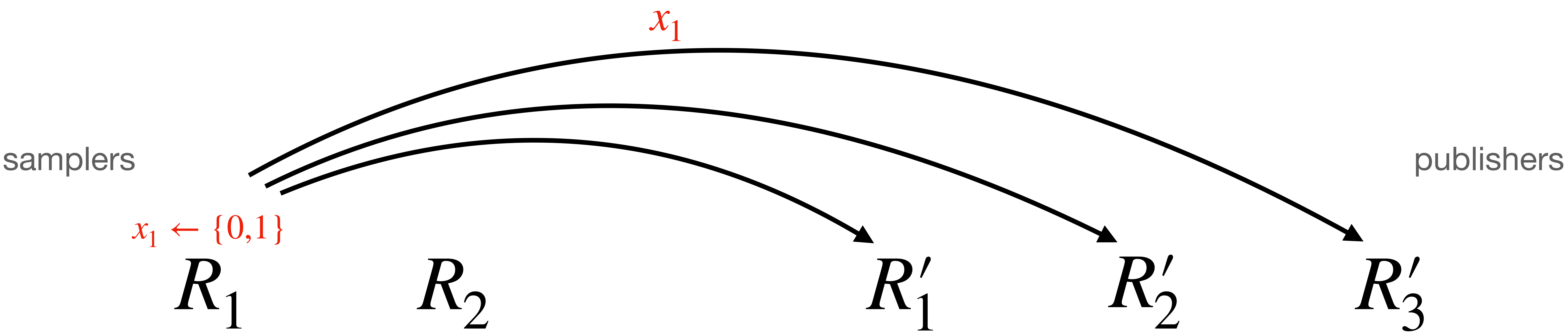
samplers

publishers

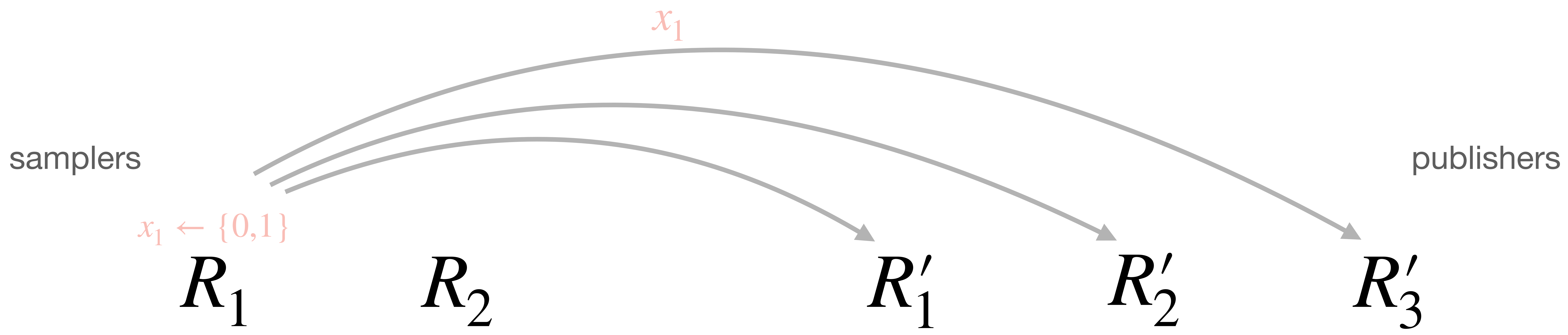
$x_1 \leftarrow \{0,1\}$

R_1 R_2 R'_1 R'_2 R'_3

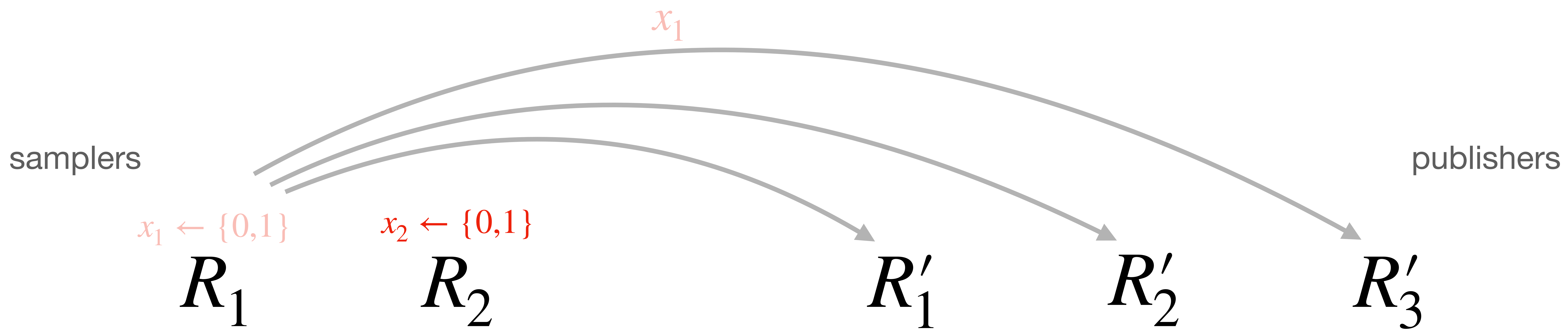
A simple improved protocol for one corruption



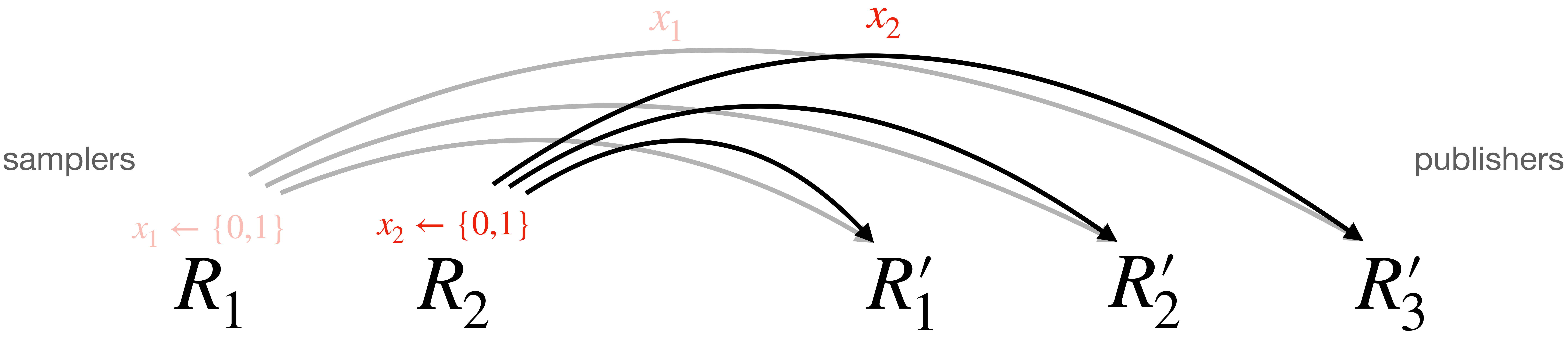
A simple improved protocol for one corruption



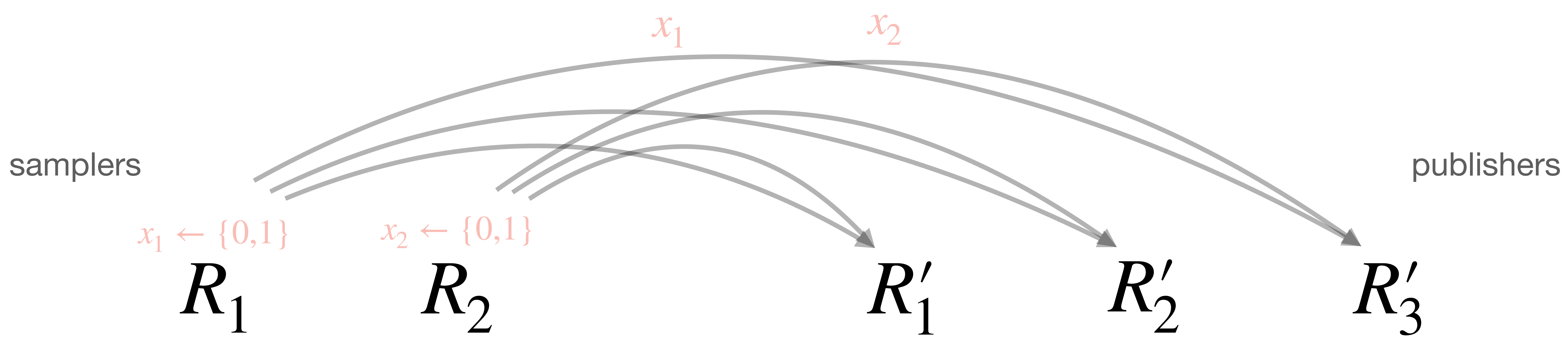
A simple improved protocol for one corruption



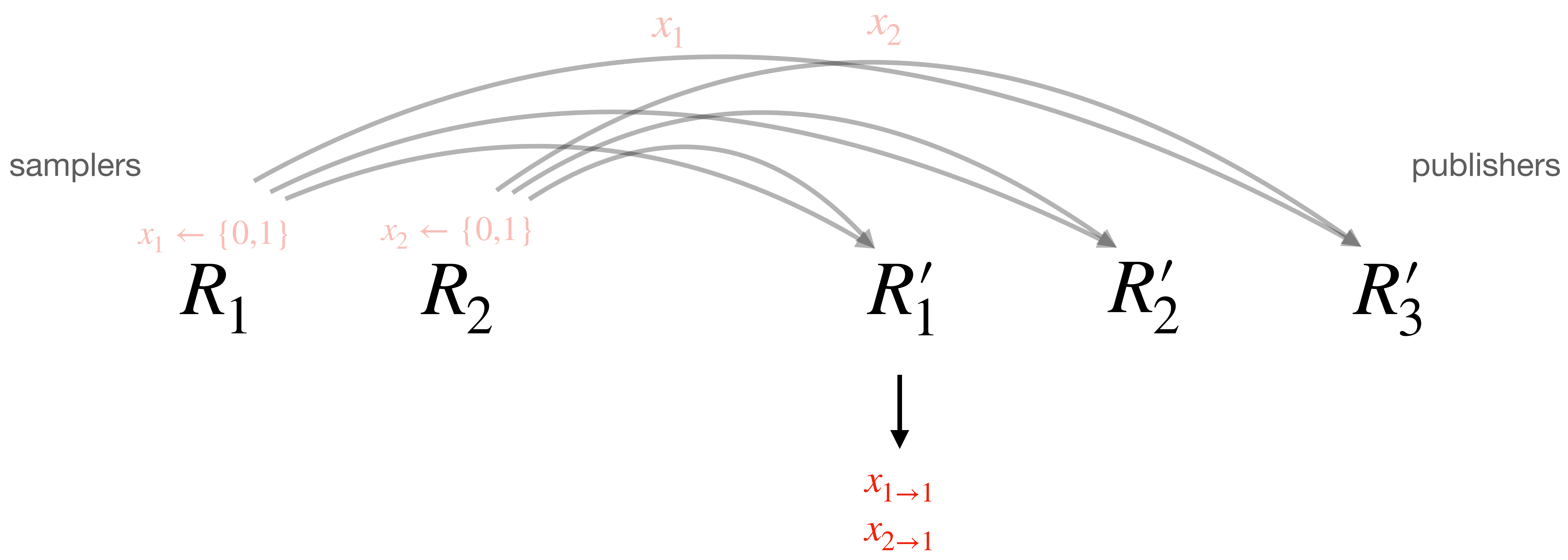
A simple improved protocol for one corruption



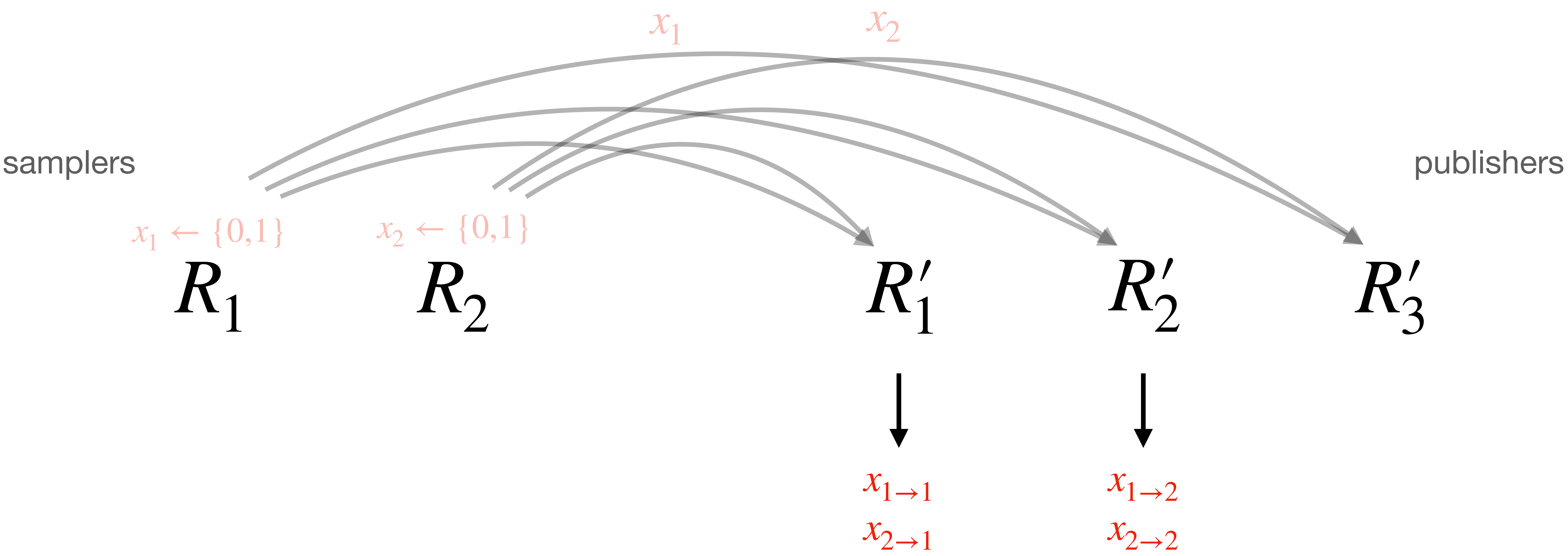
A simple improved protocol for one corruption



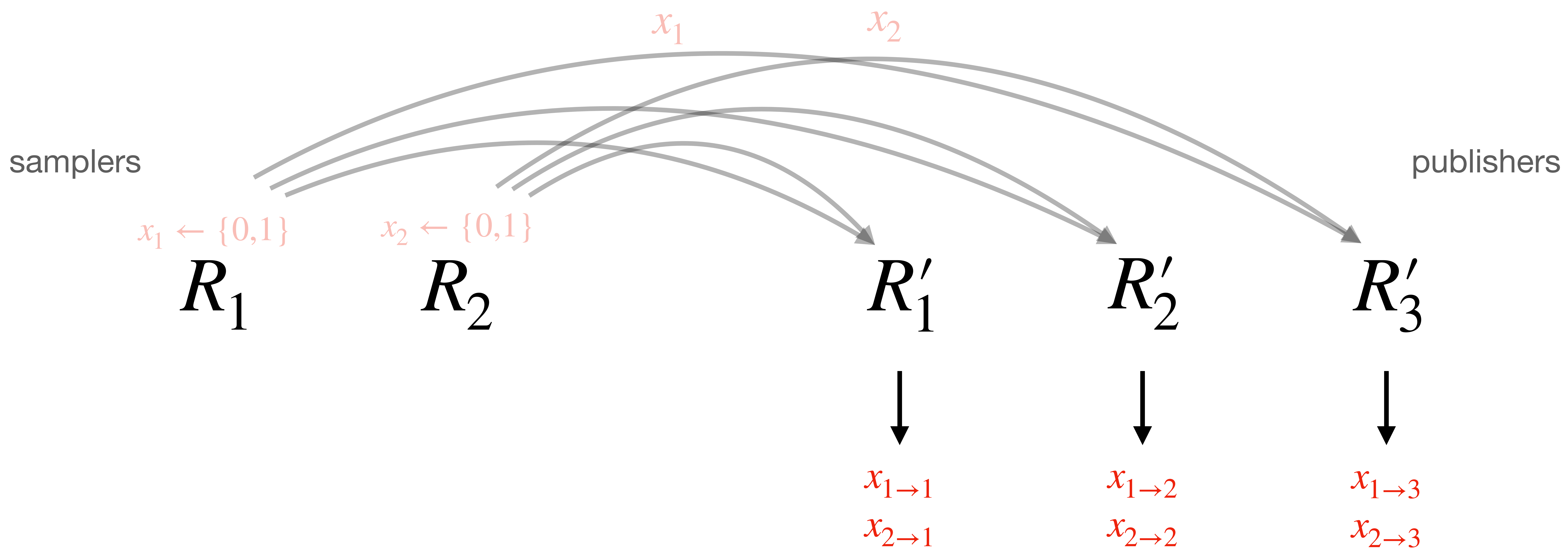
A simple improved protocol for one corruption



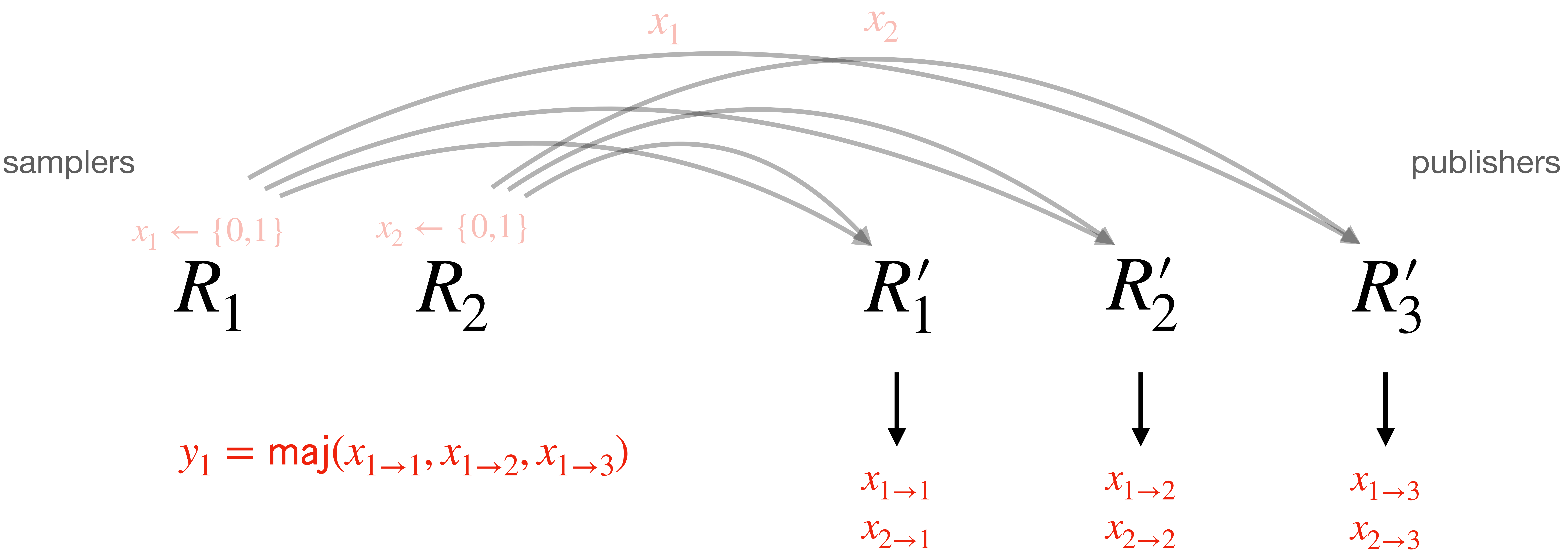
A simple improved protocol for one corruption



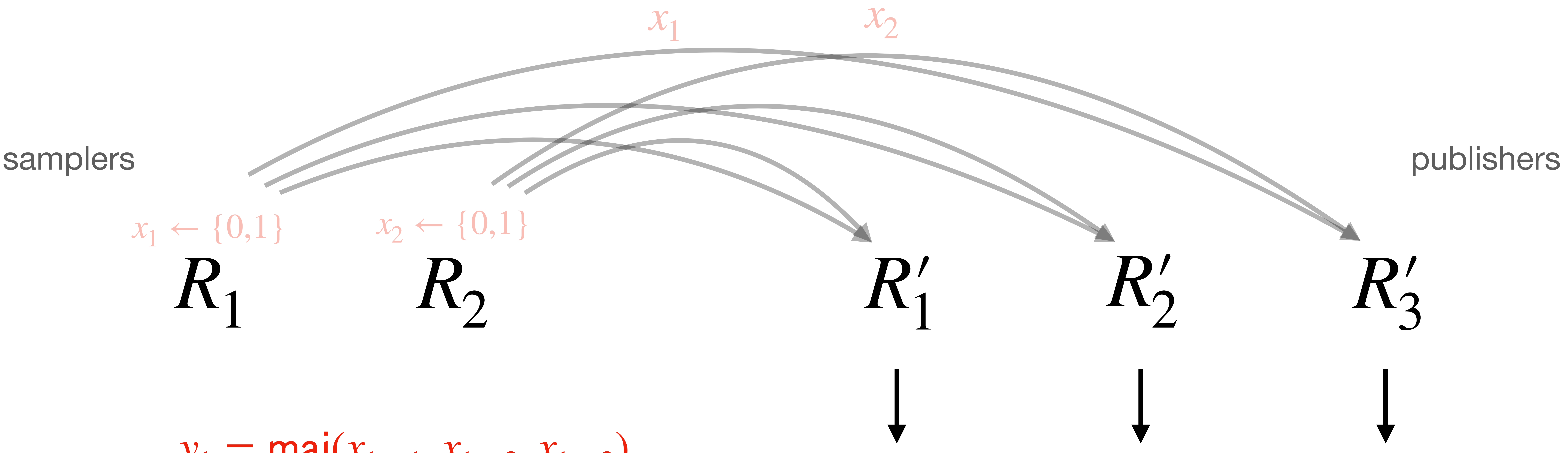
A simple improved protocol for one corruption



A simple improved protocol for one corruption



A simple improved protocol for one corruption

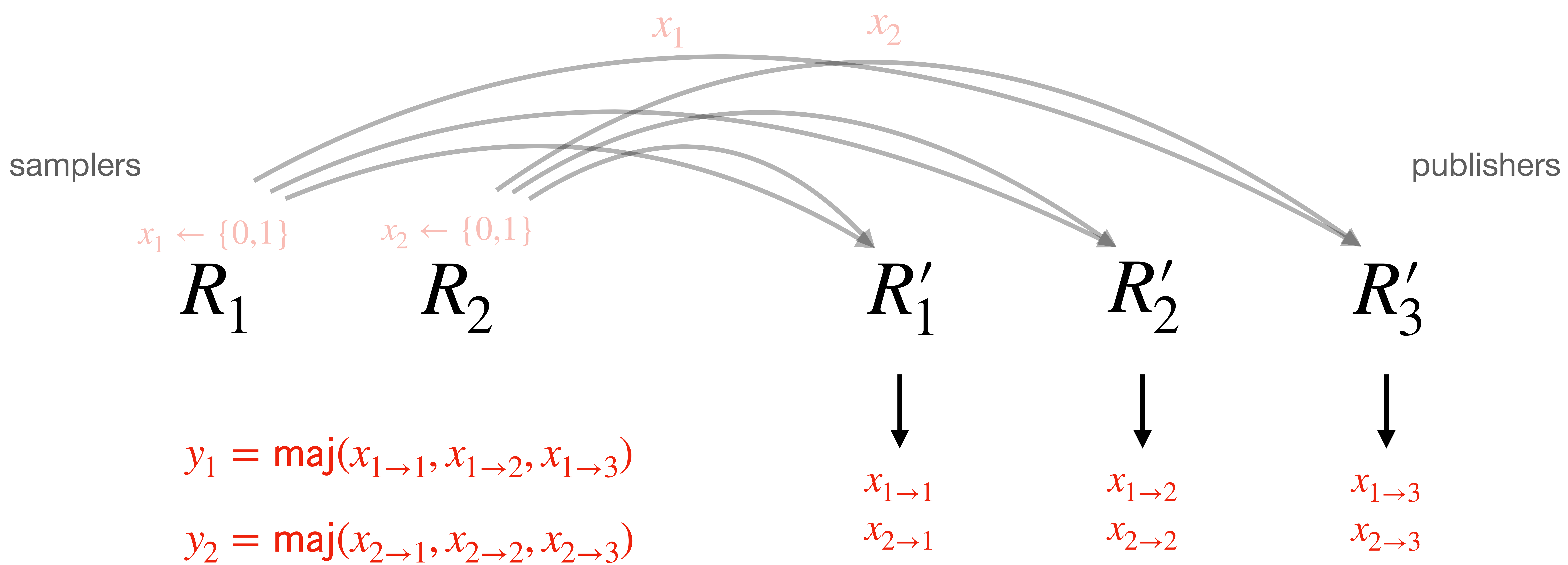


$x_{1\to 1}$	$x_{1\to 2}$	$x_{1\to 3}$
$x_{2\to 1}$	$x_{2\to 2}$	$x_{2\to 3}$

$y_1 = \text{maj}(x_{1\to 1}, x_{1\to 2}, x_{1\to 3})$

$y_2 = \text{maj}(x_{2\to 1}, x_{2\to 2}, x_{2\to 3})$

A simple improved protocol for one corruption

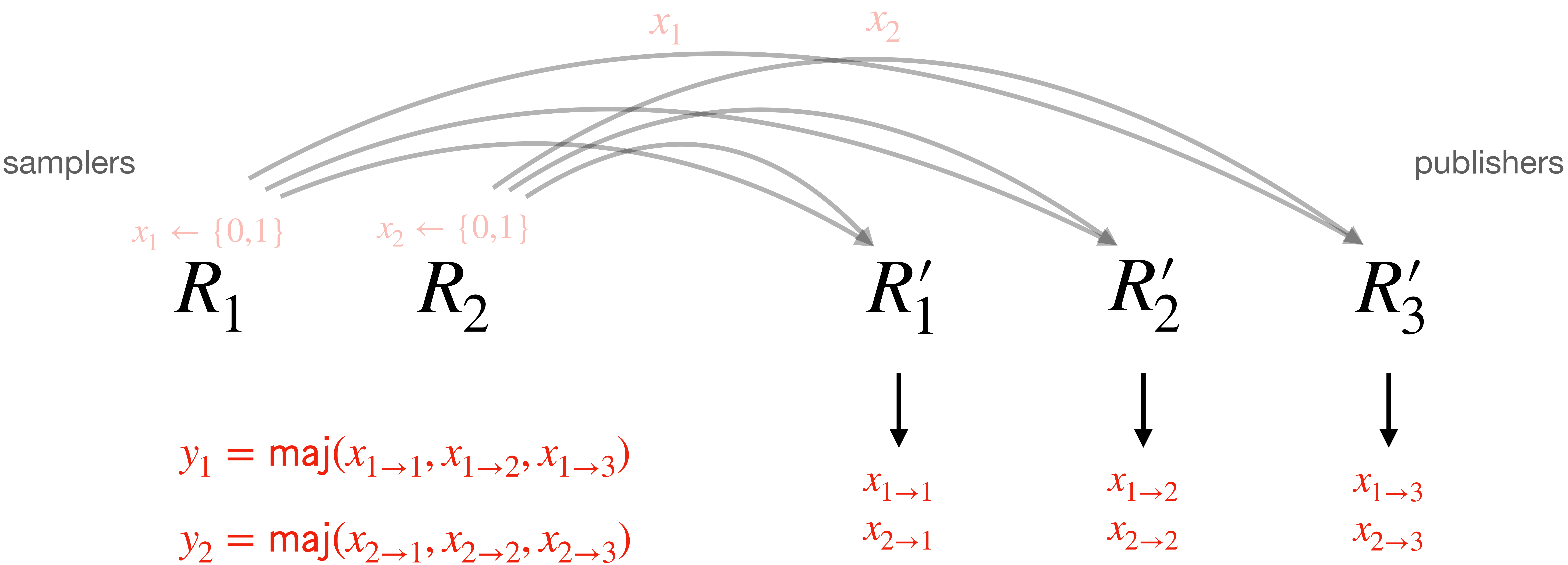


$y_1 = \mathsf{maj}(x_{1\to1}, x_{1\to2}, x_{1\to3})$

$y_2 = \mathsf{maj}(x_{2\to1}, x_{2\to2}, x_{2\to3})$

$b = y_1 \oplus y_2$

A simple improved protocol for one corruption



$y_1 = \text{maj}(x_{1\to1}, x_{1\to2}, x_{1\to3})$

$y_2 = \text{maj}(x_{2\to1}, x_{2\to2}, x_{2\to3})$

$b = y_1 \oplus y_2$

Can be generalized using $n = 5t$ roles.

Impossibility result

Every randomness extraction protocol with bias < 0.01 against t corruptions requires $n \geq 4t + 1$ roles.

Impossibility result

Every randomness extraction protocol with bias < 0.01 against t corruptions requires $n \geq 4t + 1$ roles.

$n^\star = n^\star(t) =$ Smallest number of roles for which we can handle t corruptions

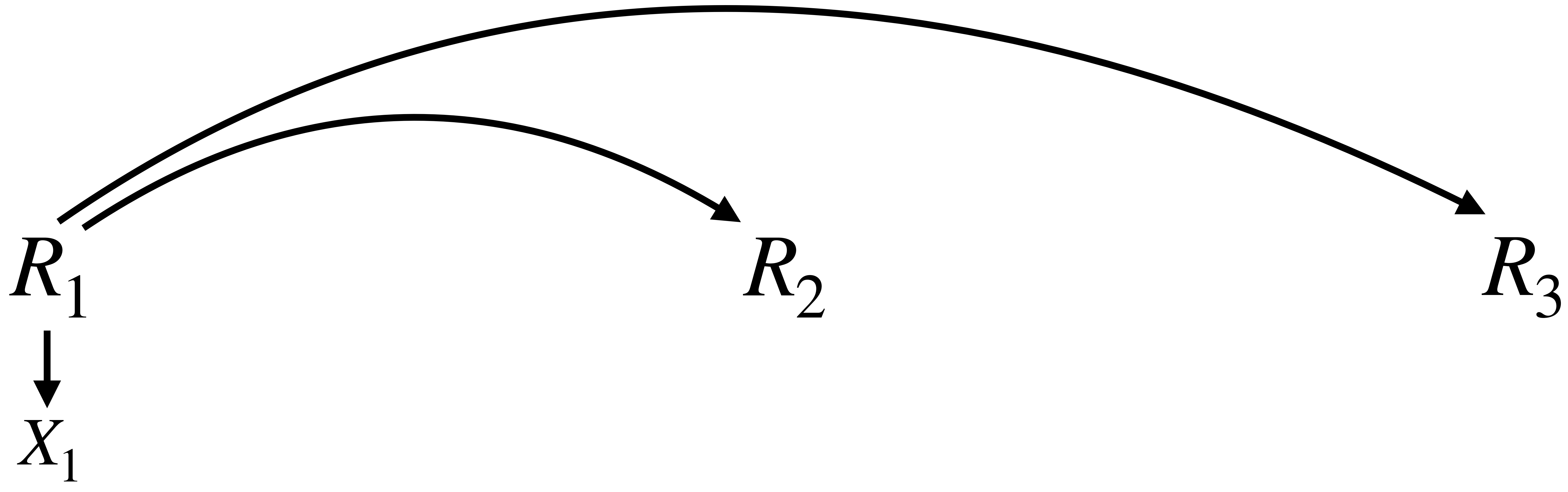
Stronger adversary: $4t + 1 \leq n^\star \leq 6t + 1$

Weaker adversary (this talk): $4t + 1 \leq n^\star \leq 5t$

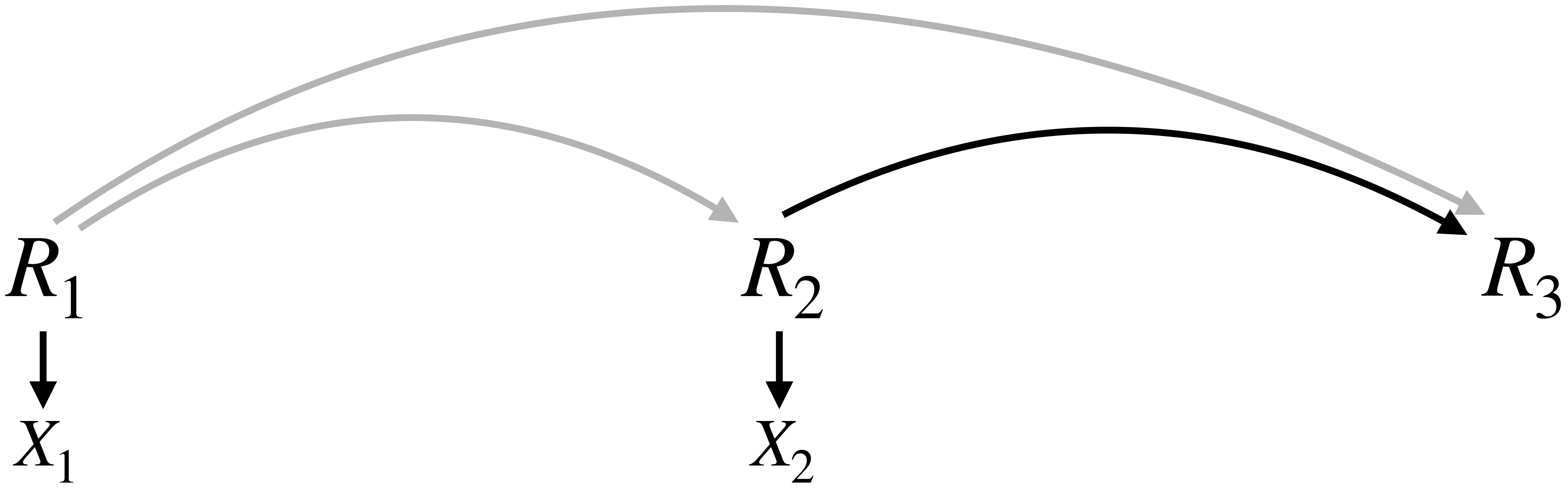
Impossibility for 3 roles, 1 corruption

R_1 R_2 R_3

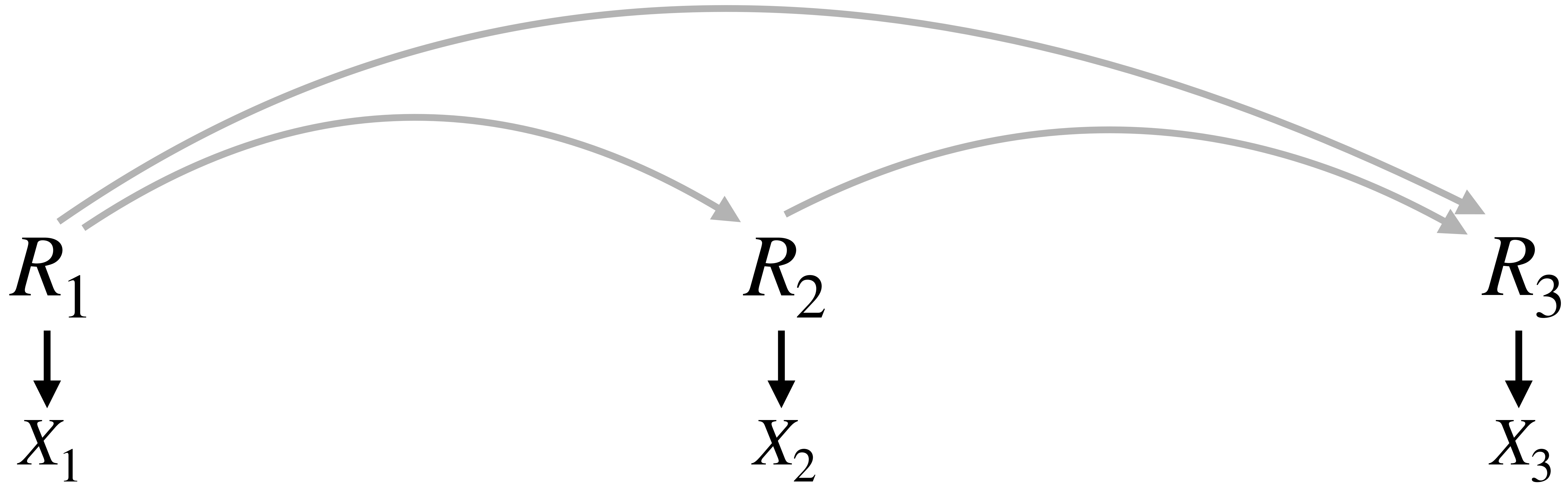
Impossibility for 3 roles, 1 corruption



Impossibility for 3 roles, 1 corruption



Impossibility for 3 roles, 1 corruption

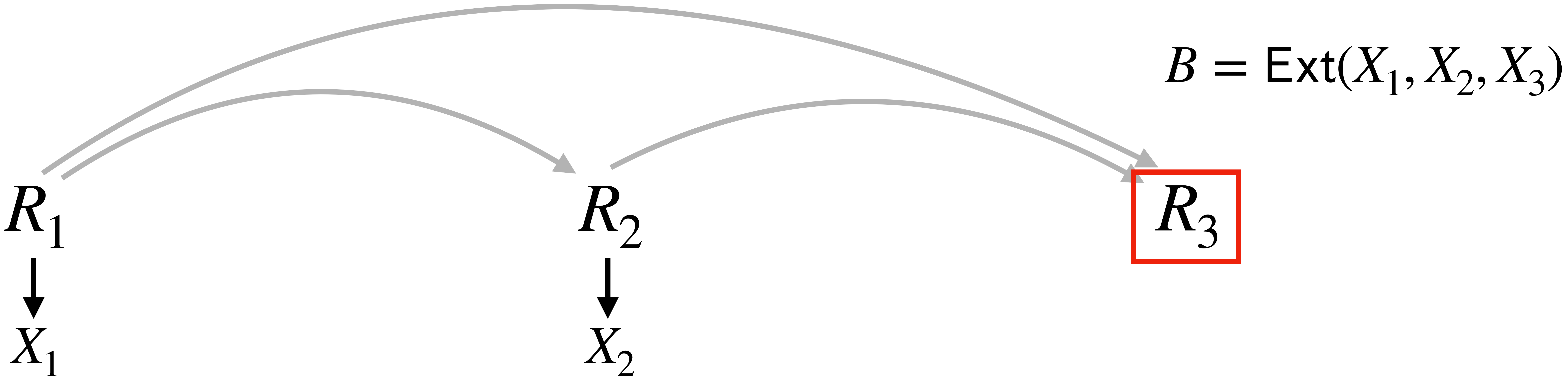


Impossibility for 3 roles, 1 corruption

$$B = \mathsf{Ext}(X_1, X_2, X_3)$$

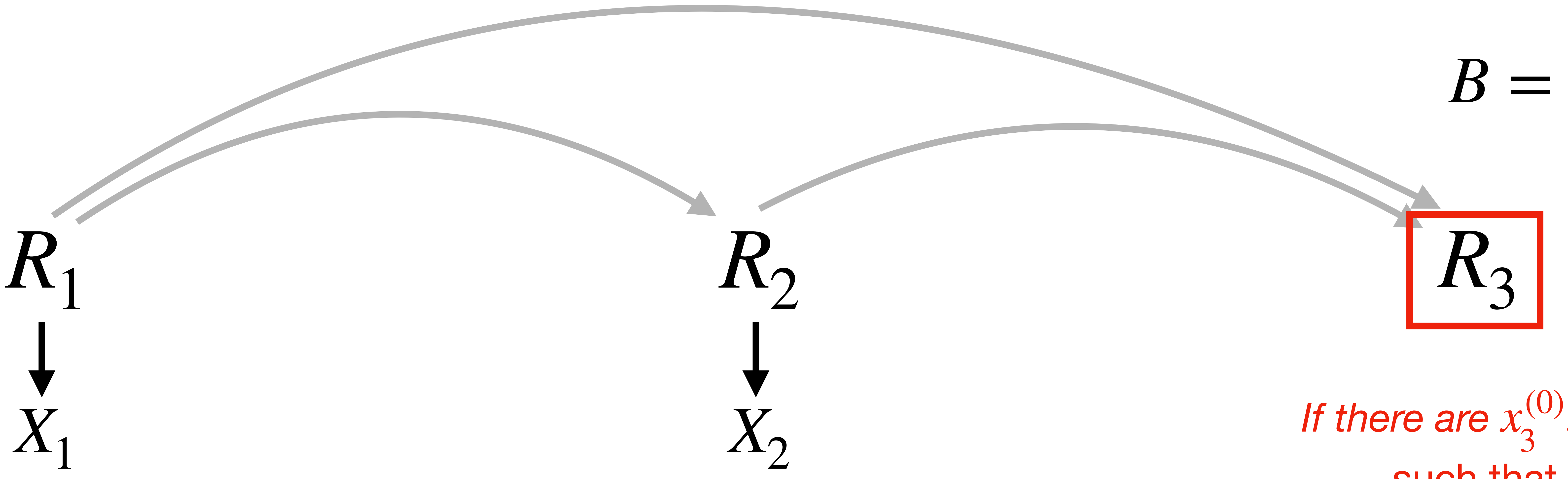
$$\begin{tikzcd}
R_1 \arrow[r, bend left] \arrow[rr, bend left] \arrow[d] & R_2 \arrow[r, bend left] \arrow[d] & R_3 \arrow[d] \\
X_1 & X_2 & X_3
\end{tikzcd}$$

Impossibility for 3 roles, 1 corruption



Impossibility for 3 roles, 1 corruption

$B = \mathsf{Ext}(X_1, X_2, X_3)$



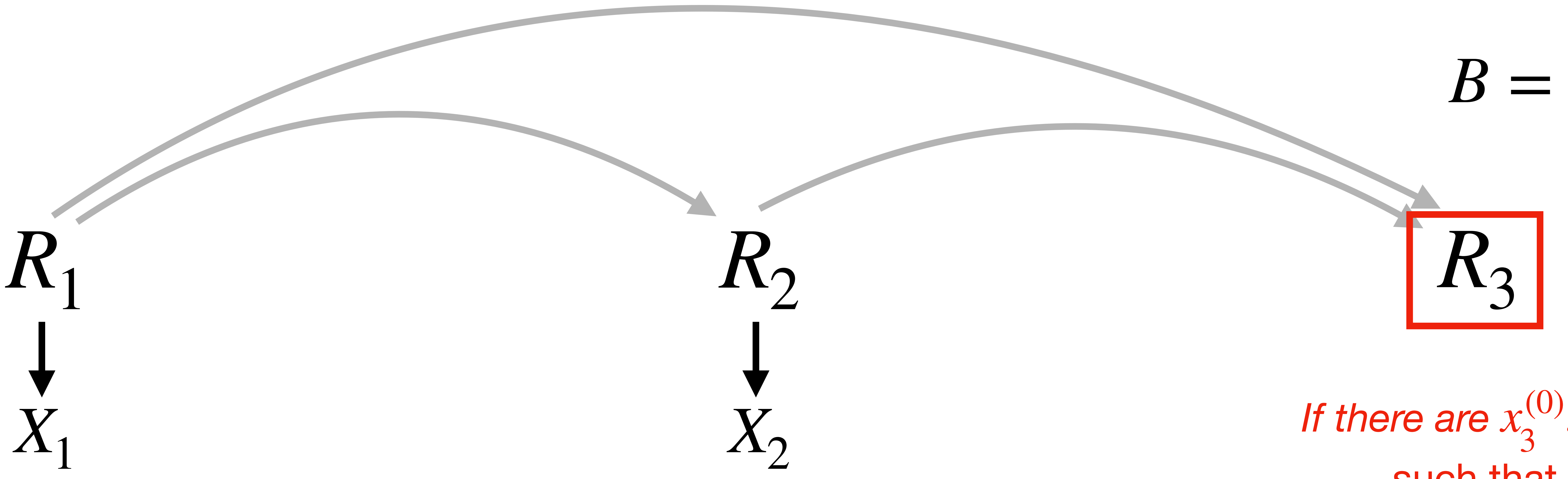
If there are $x_3^{(0)}, x_3^{(1)}$

such that

$\mathsf{Ext}(X_1, X_2, x_3^{(b)}) = b$

Impossibility for 3 roles, 1 corruption

$B = \mathsf{Ext}(X_1, X_2, X_3)$



If there are $x_3^{(0)}, x_3^{(1)}$
such that
$\mathsf{Ext}(X_1, X_2, x_3^{(b)}) = b$

Bias!

Impossibility for 3 roles, 1 corruption

$B = \text{Ext}(X_1, X_2, X_3)$

R_1 $\quad$ R_2 $\quad$ $\boxed{R_3}$

$\downarrow$ $\quad$ $\downarrow$

X_1 $\quad$ X_2

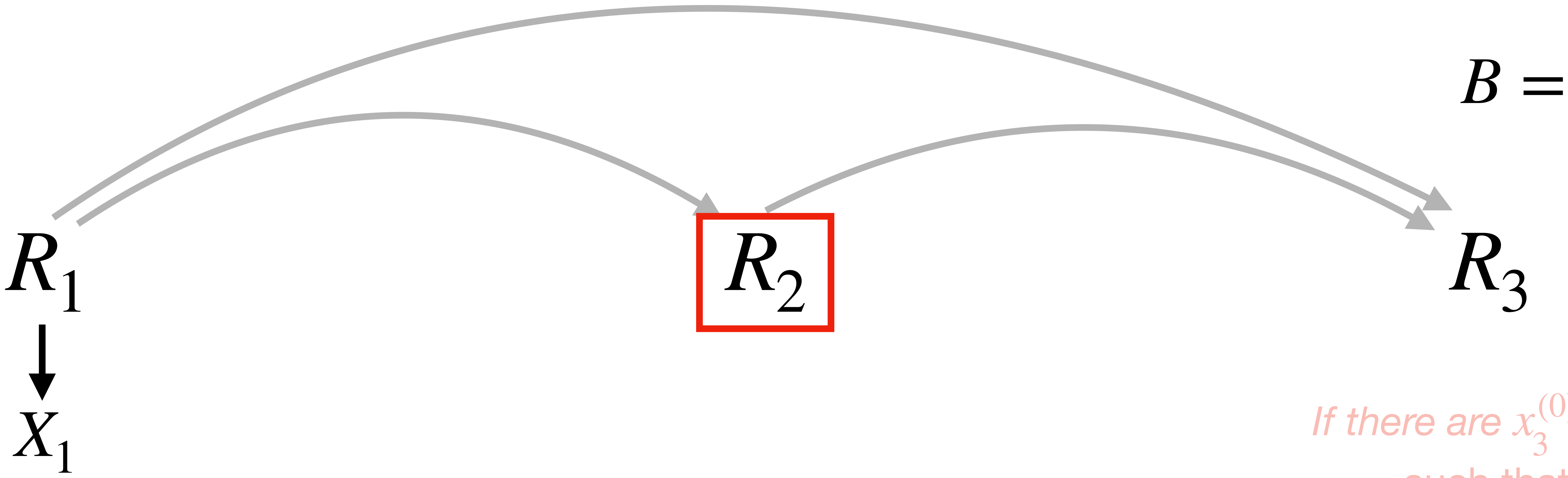
If there are $x_3^{(0)}, x_3^{(1)}$
such that
$\text{Ext}(X_1, X_2, x_3^{(b)}) = b$

Bias!

X_1, X_2 must fully determine output w/ high prob

Impossibility for 3 roles, 1 corruption

$B = \mathsf{Ext}(X_1, X_2, X_3)$



If there are $x_3^{(0)}, x_3^{(1)}$ such that $\mathsf{Ext}(X_1, X_2, x_3^{(b)}) = b$

Bias!

X_1, X_2 must fully determine output w/ high prob

Impossibility for 3 roles, 1 corruption

$B = \text{Ext}(X_1, X_2, X_3)$

R_1 $\qquad$ $\boxed{R_2}$ $\qquad$ R_3

$R_1 \to X_1$

Sample $X_2^{(0)}, X_2^{(1)} \overset{i.i.d.}{\sim} (X_2 \mid X_1, M_{1\to 2})$

If $\text{Ext}(X_1, X_2^{(0)}, \cdot\,) \not\equiv \text{Ext}(X_1, X_2^{(1)}, \cdot\,)$
and both are constant

If there are $x_3^{(0)}, x_3^{(1)}$
such that
$\text{Ext}(X_1, X_2, x_3^{(b)}) = b$

Bias!

X_1, X_2 must fully determine output w/ high prob

Impossibility for 3 roles, 1 corruption

$B = \text{Ext}(X_1, X_2, X_3)$

R_1 $\qquad$ $\boxed{R_2}$ $\qquad$ R_3

$R_1 \downarrow X_1$

Sample $X_2^{(0)}, X_2^{(1)} \overset{i.i.d.}{\sim} (X_2 \mid X_1, M_{1\to 2})$

If $\text{Ext}(X_1, X_2^{(0)}, \cdot\,) \not\equiv \text{Ext}(X_1, X_2^{(1)}, \cdot\,)$
and both are constant

Bias!

If there are $x_3^{(0)}, x_3^{(1)}$
such that
$\text{Ext}(X_1, X_2, x_3^{(b)}) = b$

Bias!

X_1, X_2 must fully determine output w/ high prob

Impossibility for 3 roles, 1 corruption

$B = \text{Ext}(X_1, X_2, X_3)$

R_1 $\boxed{R_2}$ R_3

$R_1 \downarrow X_1$

Sample $X_2^{(0)}, X_2^{(1)} \overset{i.i.d.}{\sim} (X_2 \mid X_1, M_{1\to 2})$

If $\text{Ext}(X_1, X_2^{(0)}, \cdot\,) \not\equiv \text{Ext}(X_1, X_2^{(1)}, \cdot\,)$
and both are constant

Bias!

If there are $x_3^{(0)}, x_3^{(1)}$
such that
$\text{Ext}(X_1, X_2, x_3^{(b)}) = b$

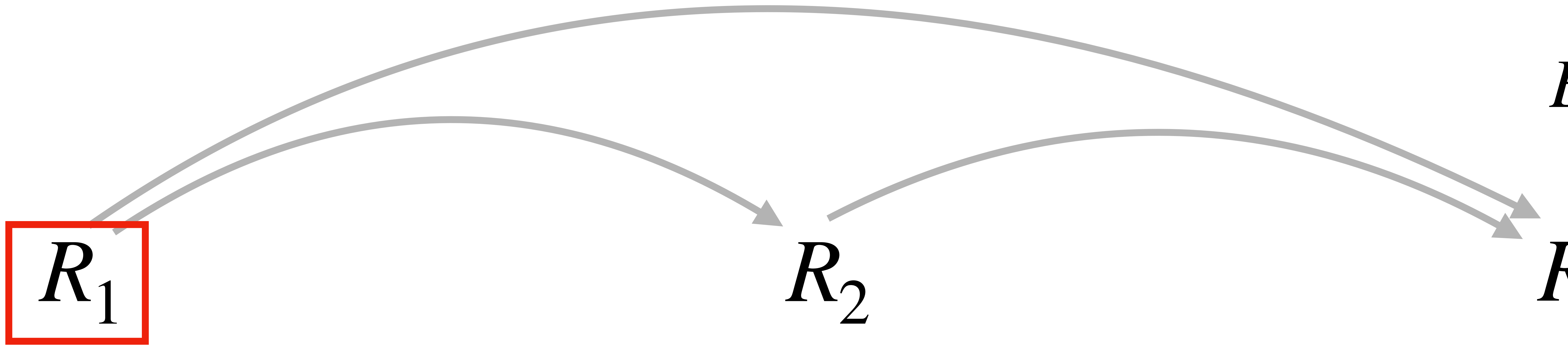
Bias!

W/ high prob over sampling
$X_2^{(0)}, X_2^{(1)} \overset{i.i.d.}{\sim} (X_2 \mid X_1, M_{1\to 2})$
must have
$\text{Ext}(X_1, X_2^{(0)}, \cdot\,) \equiv \text{Ext}(X_1, X_2^{(1)}, \cdot\,)$

X_1, X_2 ***must fully determine output w/ high prob***

Impossibility for 3 roles, 1 corruption

$B = \mathsf{Ext}(X_1, X_2, X_3)$



Sample $X_2^{(0)}, X_2^{(1)} \overset{i.i.d.}{\sim} (X_2 \mid X_1, M_{1\to 2})$

If $\mathsf{Ext}(X_1, X_2^{(0)}, \cdot\,) \not\equiv \mathsf{Ext}(X_1, X_2^{(1)}, \cdot\,)$
and both are constant

Bias!

If there are $x_3^{(0)}, x_3^{(1)}$
such that
$\mathsf{Ext}(X_1, X_2, x_3^{(b)}) = b$

Bias!

W/ high prob over sampling
$X_2^{(0)}, X_2^{(1)} \overset{i.i.d.}{\sim} (X_2 \mid X_1, M_{1\to 2})$
must have
$\mathsf{Ext}(X_1, X_2^{(0)}, \cdot\,) \equiv \mathsf{Ext}(X_1, X_2^{(1)}, \cdot\,)$

X_1, X_2 ***must fully determine output w/ high prob***

Impossibility for 3 roles, 1 corruption

$B = \mathsf{Ext}(X_1, X_2, X_3)$

$\boxed{R_1}$ R_2 R_3

Sample $X_1^{(0)}, X_1^{(1)} \overset{i.i.d.}{\sim} X_1$
With prob $\approx 1/2$ *lead to different coin values and* R_1 *can predict values w/ high prob*

Sample $X_2^{(0)}, X_2^{(1)} \overset{i.i.d.}{\sim} (X_2 \mid X_1, M_{1\to 2})$

If $\mathsf{Ext}(X_1, X_2^{(0)}, \cdot\,) \not\equiv \mathsf{Ext}(X_1, X_2^{(1)}, \cdot\,)$ and both are constant

Bias!

If there are $x_3^{(0)}, x_3^{(1)}$ such that $\mathsf{Ext}(X_1, X_2, x_3^{(b)}) = b$

Bias!

W/ high prob over sampling $X_2^{(0)}, X_2^{(1)} \overset{i.i.d.}{\sim} (X_2 \mid X_1, M_{1\to 2})$ ***must have*** $\mathsf{Ext}(X_1, X_2^{(0)}, \cdot\,) \equiv \mathsf{Ext}(X_1, X_2^{(1)}, \cdot\,)$

X_1, X_2 ***must fully determine output w/ high prob***

Impossibility for 3 roles, 1 corruption

$B = \text{Ext}(X_1, X_2, X_3)$

R_1 $\quad$ R_2 $\quad$ R_3

Sample $X_1^{(0)}, X_1^{(1)} \overset{i.i.d.}{\sim} X_1$

With prob $\approx 1/2$ *lead to different coin values and* R_1 *can predict values w/ high prob*

Bias!

Sample $X_2^{(0)}, X_2^{(1)} \overset{i.i.d.}{\sim} (X_2 \,|\, X_1, M_{1\to 2})$

If $\text{Ext}(X_1, X_2^{(0)}, \cdot\,) \not\equiv \text{Ext}(X_1, X_2^{(1)}, \cdot\,)$ and both are constant

Bias!

If there are $x_3^{(0)}, x_3^{(1)}$ such that $\text{Ext}(X_1, X_2, x_3^{(b)}) = b$

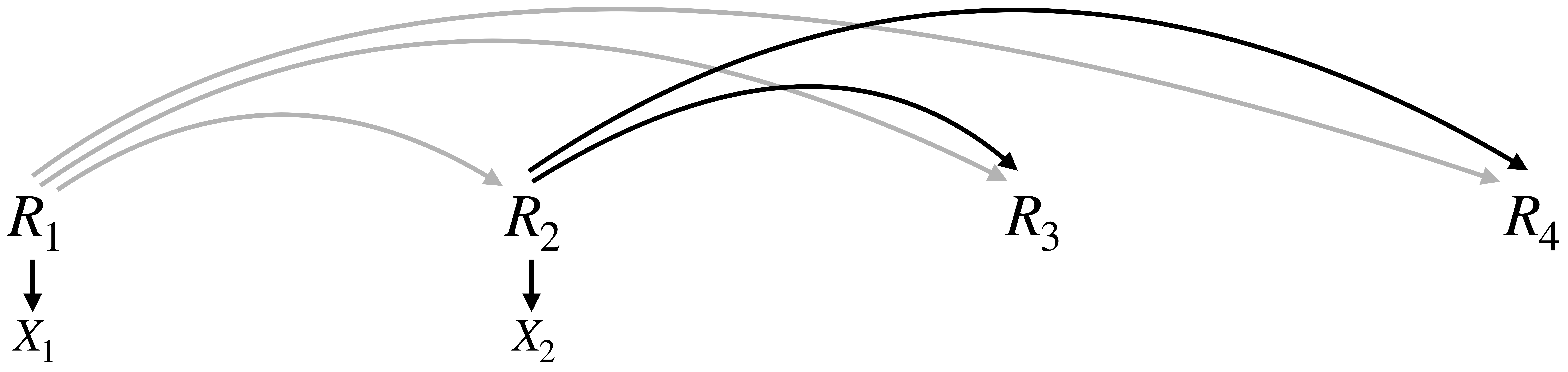
Bias!

W/ high prob over sampling
$X_2^{(0)}, X_2^{(1)} \overset{i.i.d.}{\sim} (X_2 \,|\, X_1, M_{1\to 2})$
must have
$\text{Ext}(X_1, X_2^{(0)}, \cdot\,) \equiv \text{Ext}(X_1, X_2^{(1)}, \cdot\,)$

X_1, X_2 ***must fully determine output w/ high prob***

Impossibility for 4 roles, 1 corruption

Impossibility for 4 roles, 1 corruption



Impossibility for 4 roles, 1 corruption

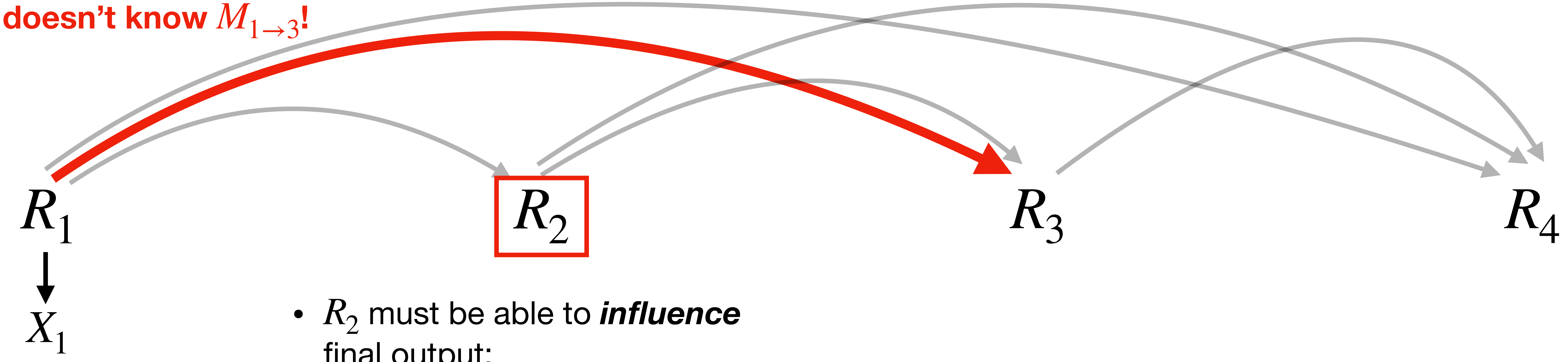
Impossibility for 4 roles, 1 corruption

Impossibility for 4 roles, 1 corruption

- R_2 must be able to ***influence*** final output;
- R_2 must be able to ***predict*** which path leads to each value.

Impossibility for 4 roles, 1 corruption

R_2 **doesn't know** $M_{1\to 3}$**!**



- R_2 must be able to ***influence*** final output;
- R_2 must be able to ***predict*** which path leads to each value.

Concluding

- YOSO: Stateless MPC, avoids denial-of-service attacks
- Public randomness extraction in YOSO with **worst-case corruptions**:
  - Still secure if role selection mechanism is biased
  - Go beyond round-based MPC techniques
  - Related to prior work on multi-source randomness extraction

Stronger adversary: $4t + 1 \leq n^{\star} \leq 6t + 1$

Weaker adversary: $4t + 1 \leq n^{\star} \leq 5t$

Concluding

- YOSO: Stateless MPC, avoids denial-of-service attacks
- Public randomness extraction in YOSO with **worst-case corruptions**:
  - Still secure if role selection mechanism is biased
  - Go beyond round-based MPC techniques
  - Related to prior work on multi-source randomness extraction

Stronger adversary: $4t + 1 \leq n^\star \leq 6t + 1$

Weaker adversary: $4t + 1 \leq n^\star \leq 5t$

Open problems:

- Close gap between our upper and lower bounds
- Protocols with communication complexity poly(n)
- More functionalities!

Concluding

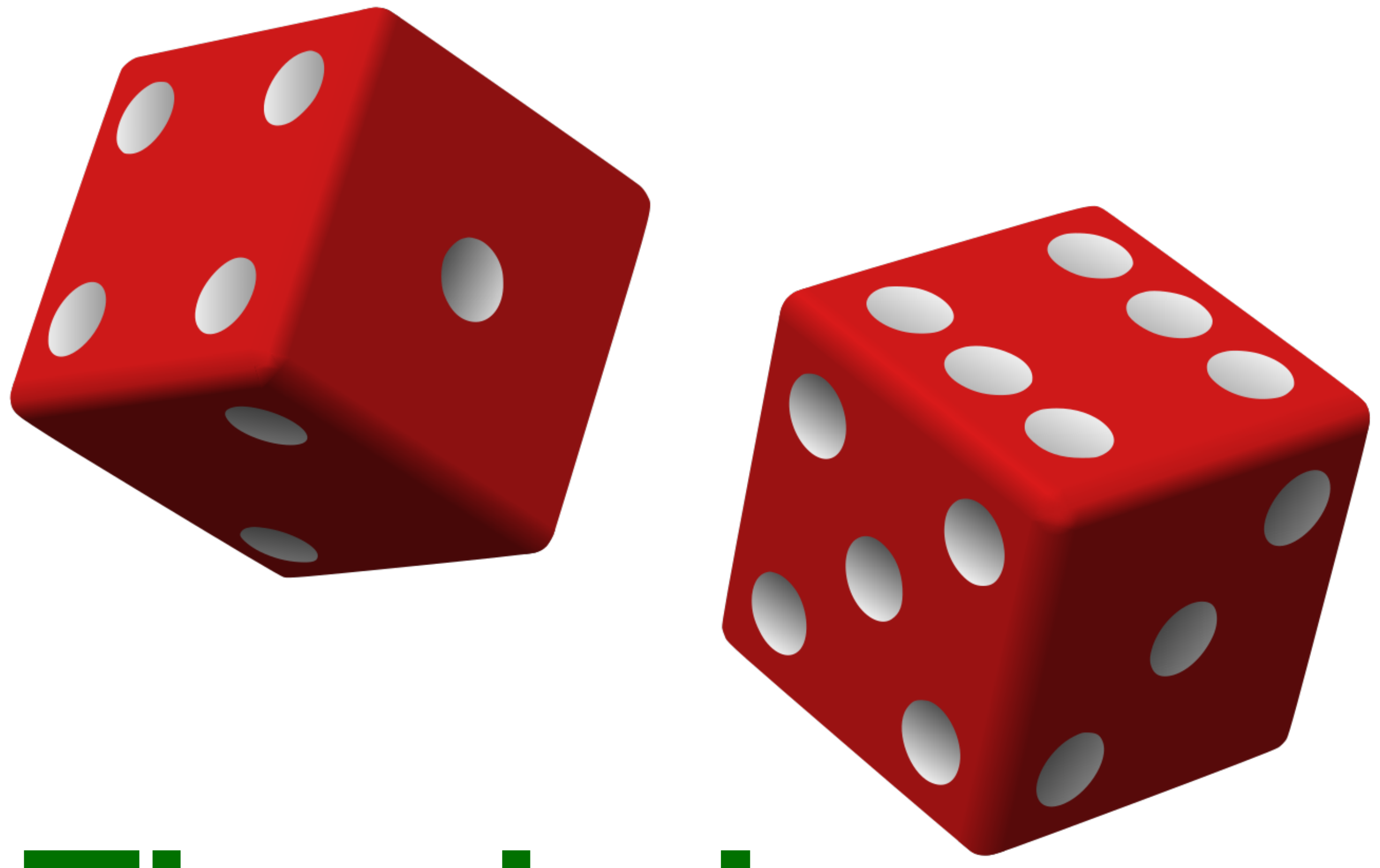
- YOSO: Stateless MPC, avoids denial-of-service attacks
- Public randomness extraction in YOSO with **worst-case corruptions**:
  - Still secure if role selection mechanism is biased
  - Go beyond round-based MPC techniques
  - Related to prior work on multi-source randomness extraction

Stronger adversary: $4t + 1 \leq n^\star \leq 6t + 1$

Weaker adversary: $4t + 1 \leq n^\star \leq 5t$

Open problems:

- Close gap between our upper and lower bounds
- Protocols with communication complexity poly(n)
- More functionalities!



Thanks!