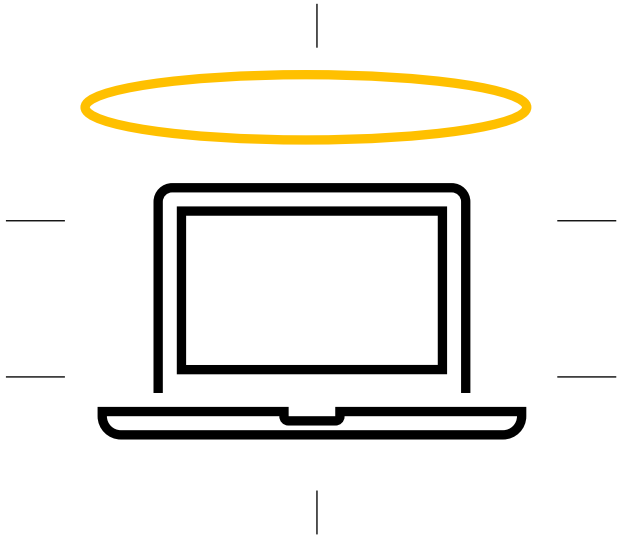
Adaptive Security of Multi-Party Protocols, Revisited

Martin Hirt
ETH Zurich

Chen-Da Liu Zhang
NTT Research

Ueli Maurer
ETH Zurich

Security Definitions



Simple

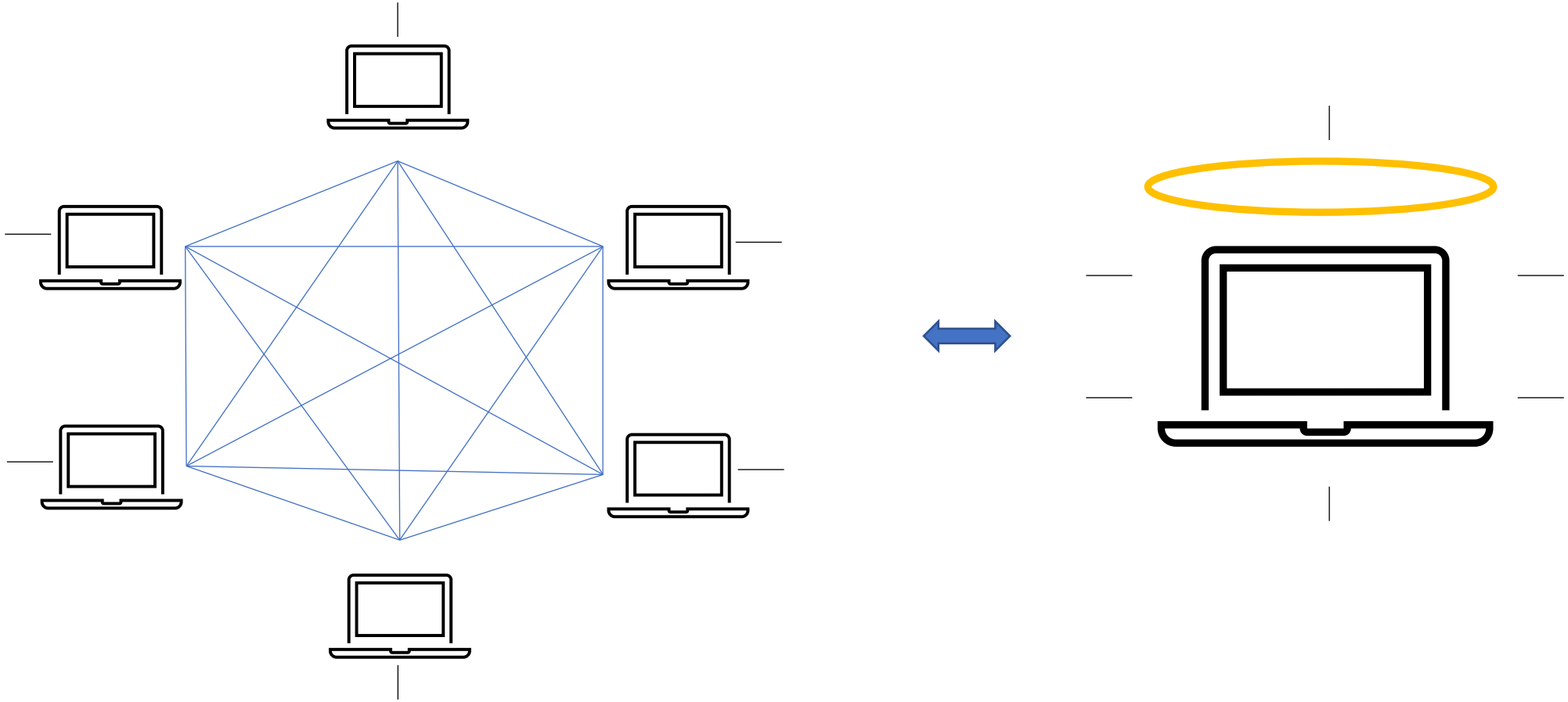
Consistent

Composable

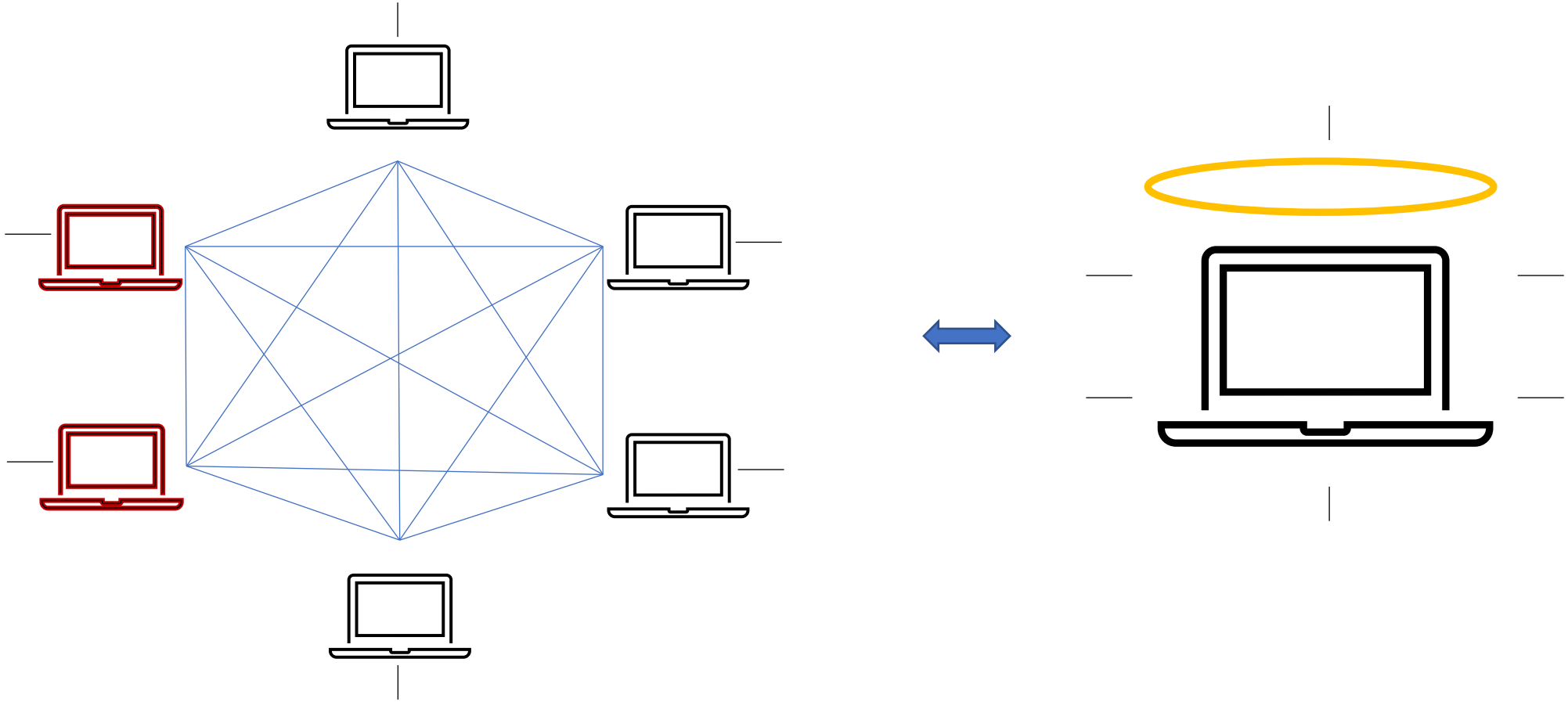
Complete

Sound

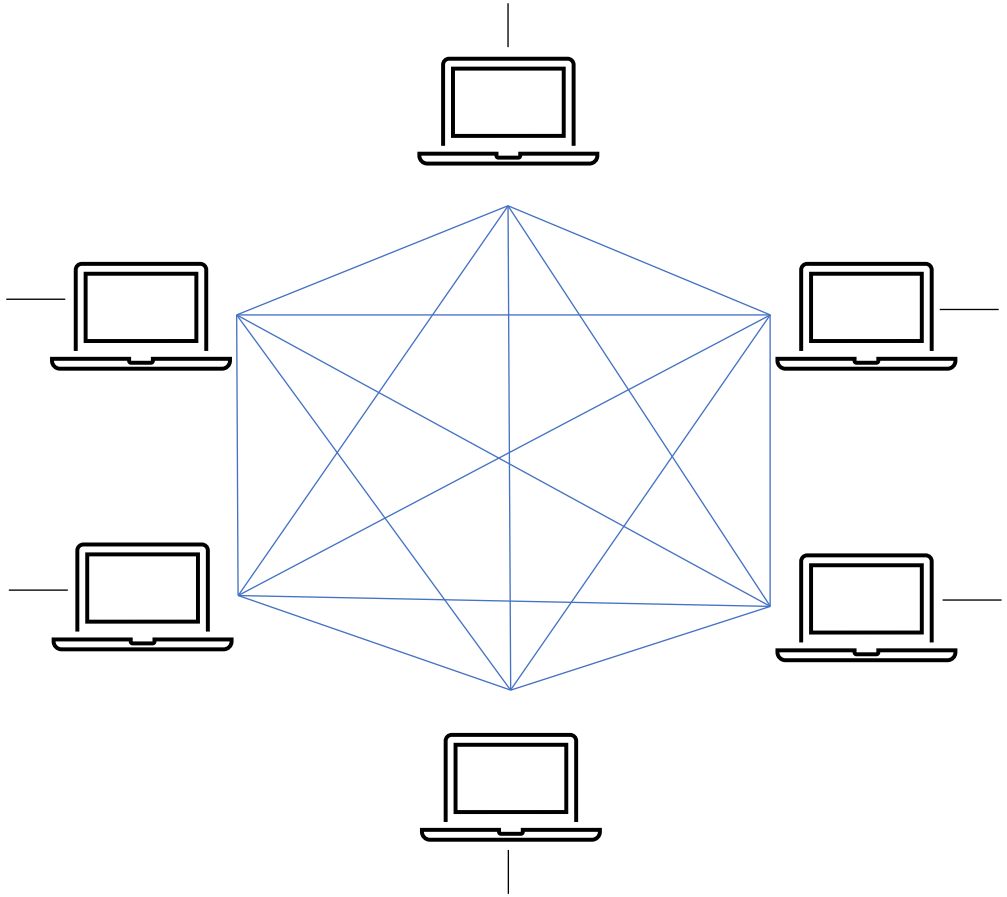
Multiparty Computation



Multiparty Computation



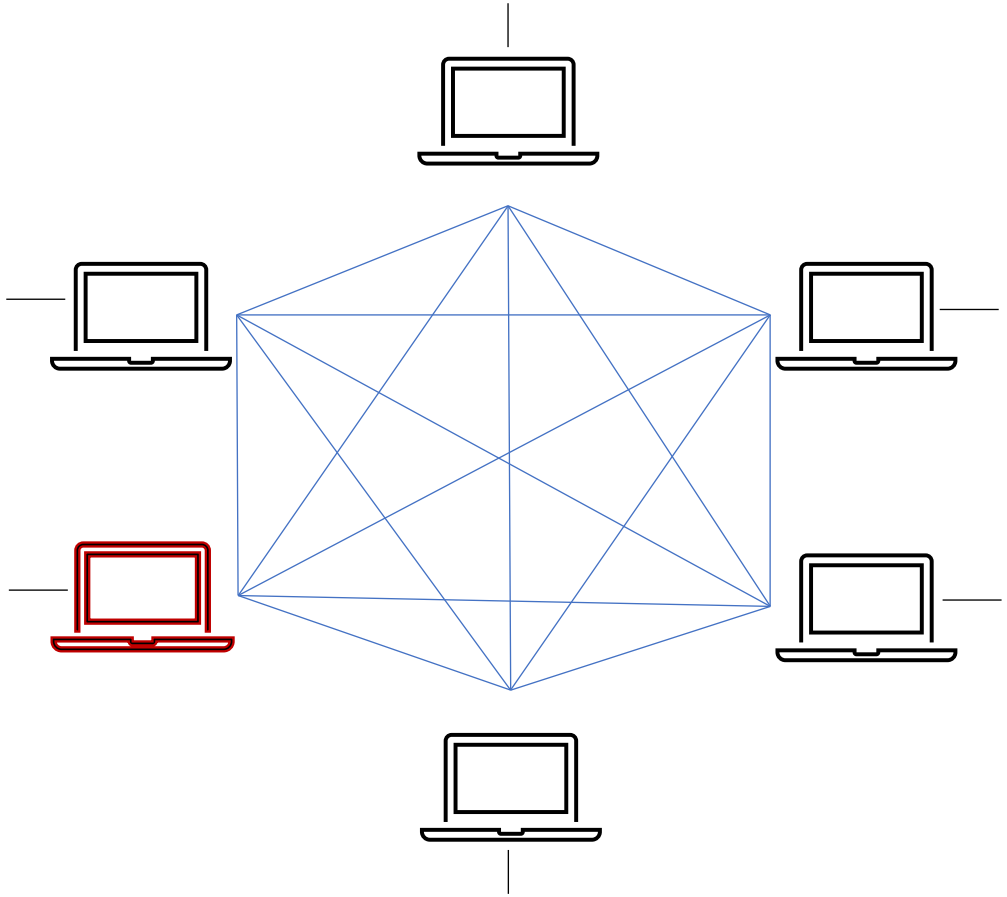
Adaptive Corruption



Network information

Internal state information

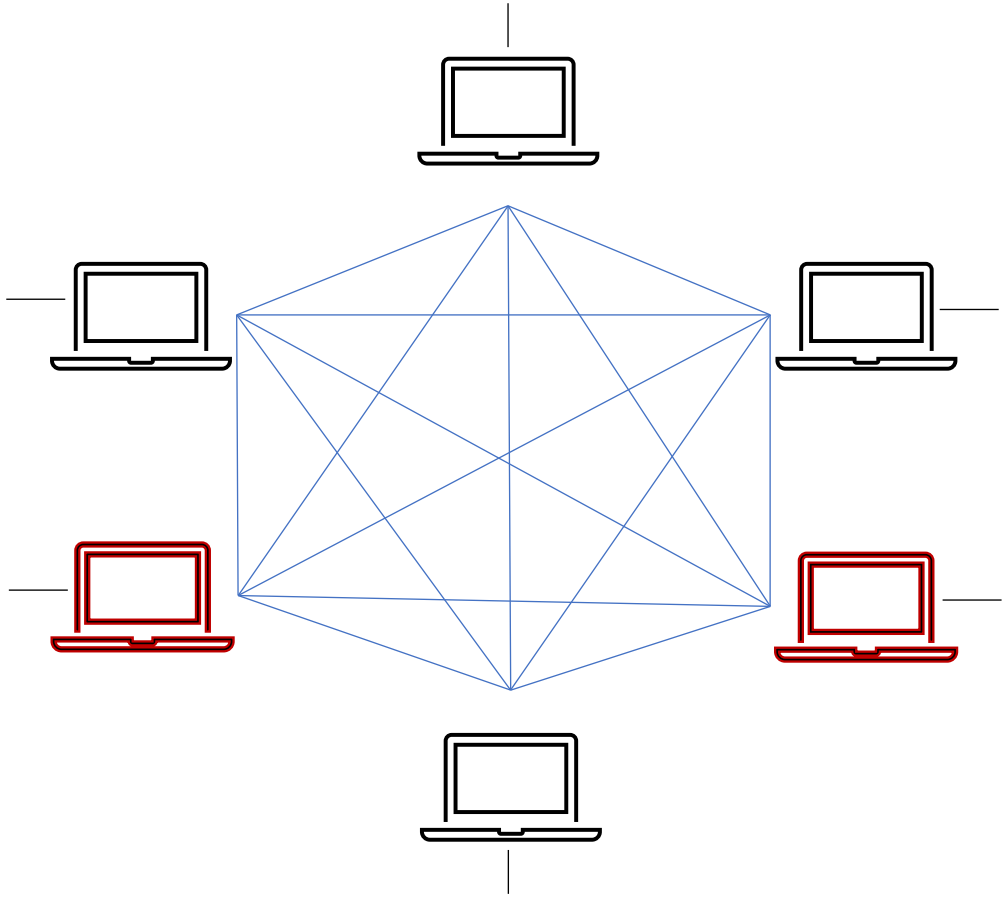
Adaptive Corruption



Network information

Internal state information

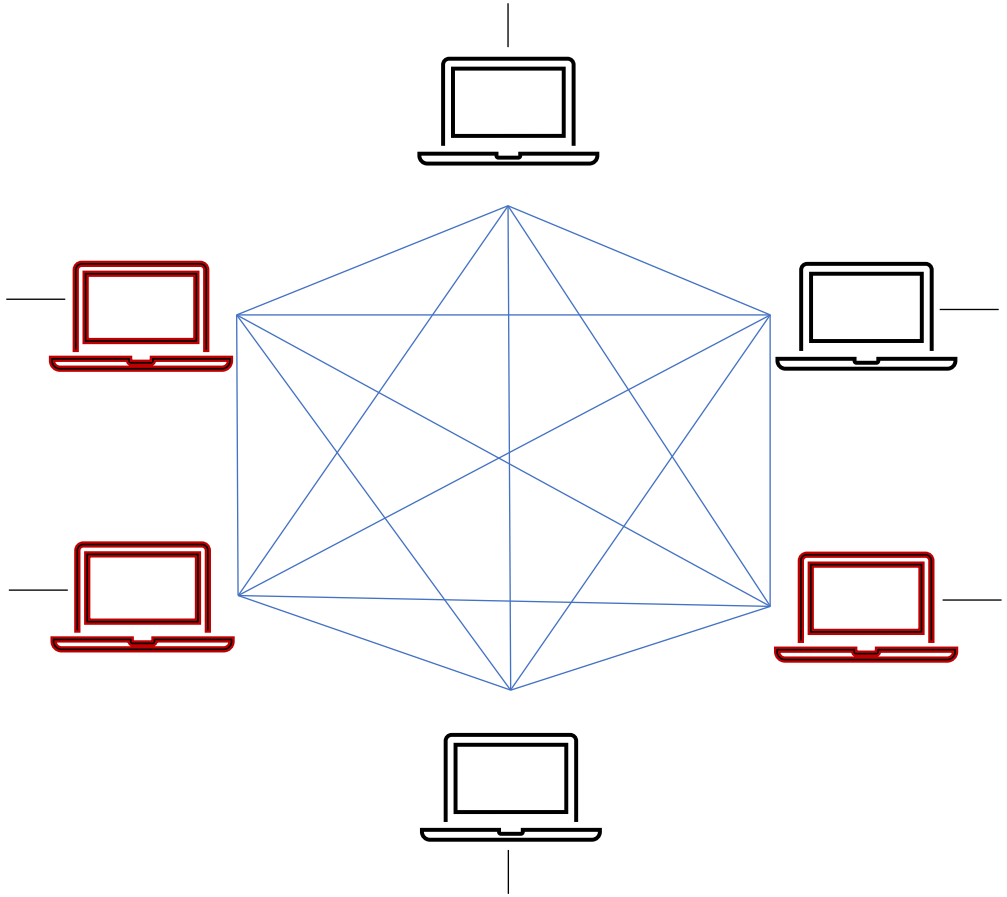
Adaptive Corruption



Network information

Internal state information

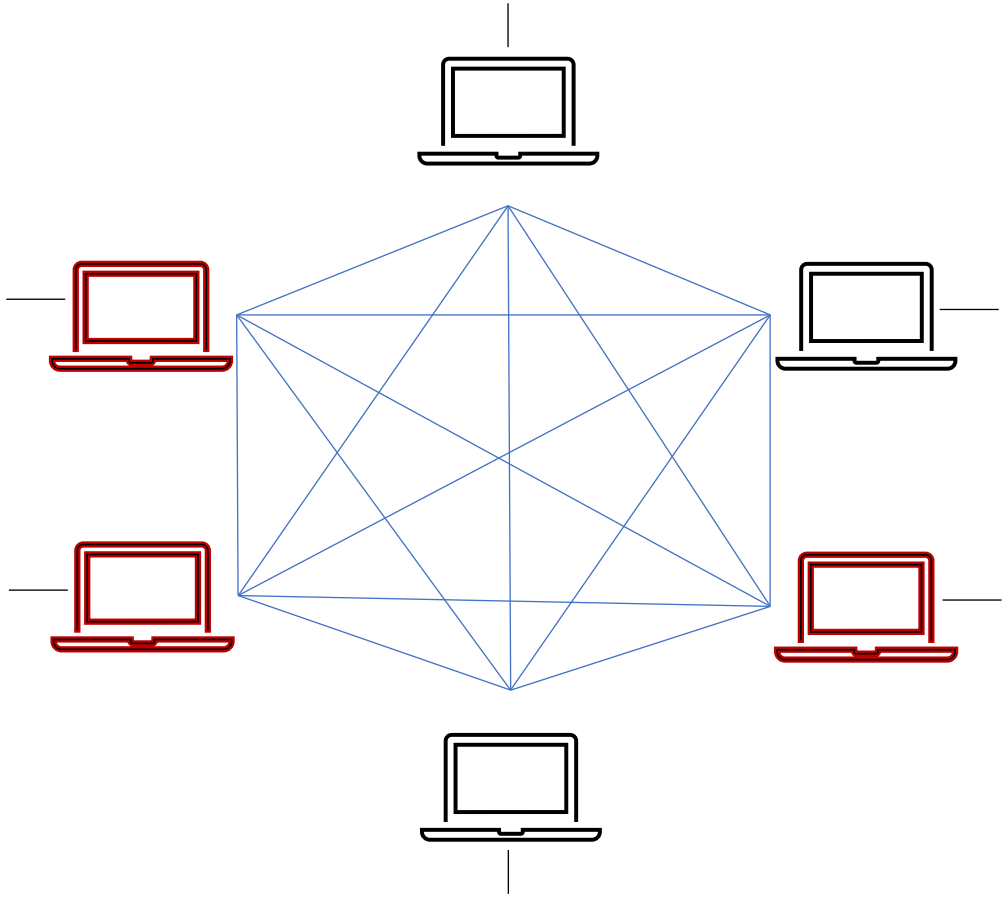
Adaptive Corruption



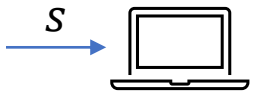
Network information

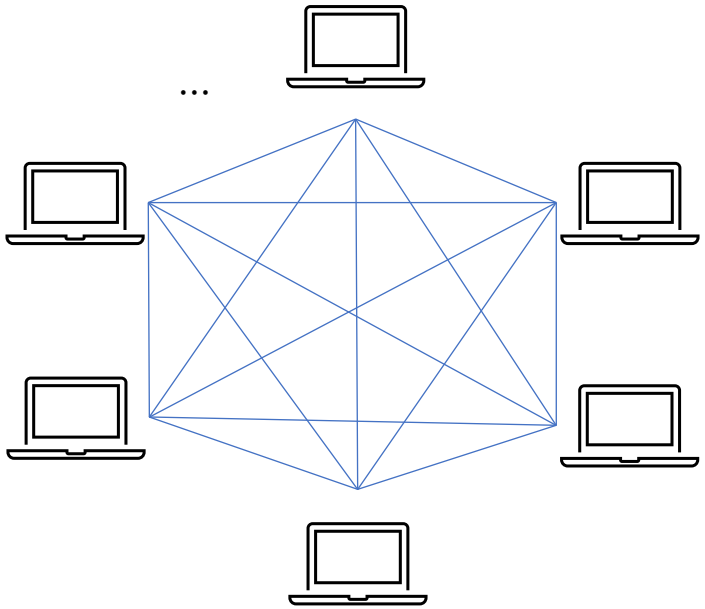
Internal state information

Adaptive Corruption

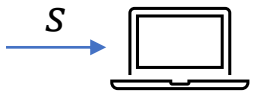


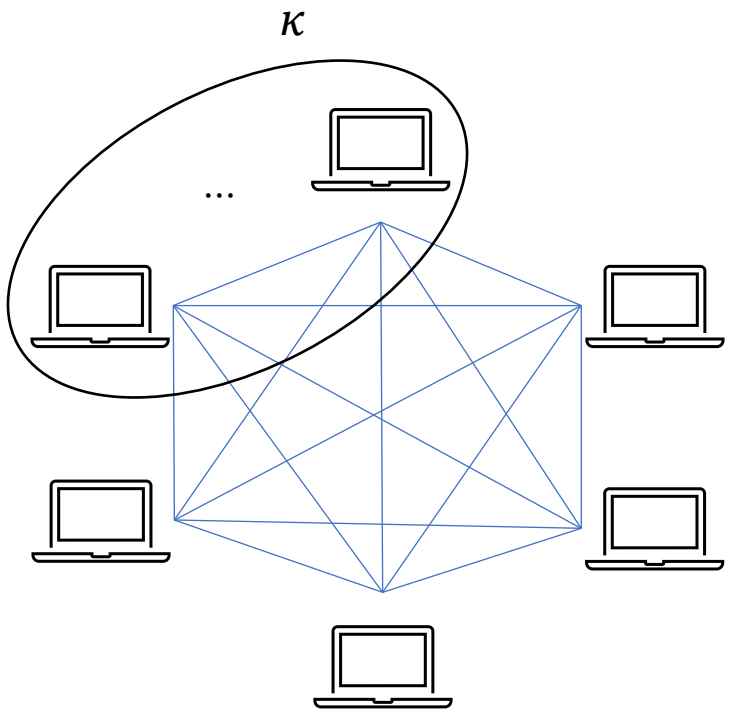
A Simple Example



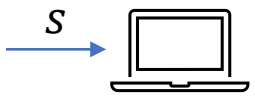


A Simple Example

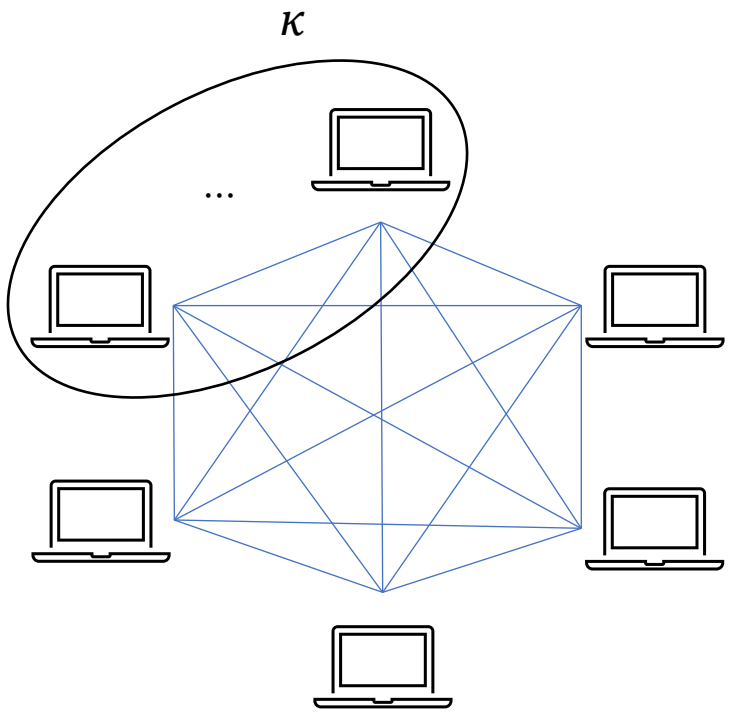




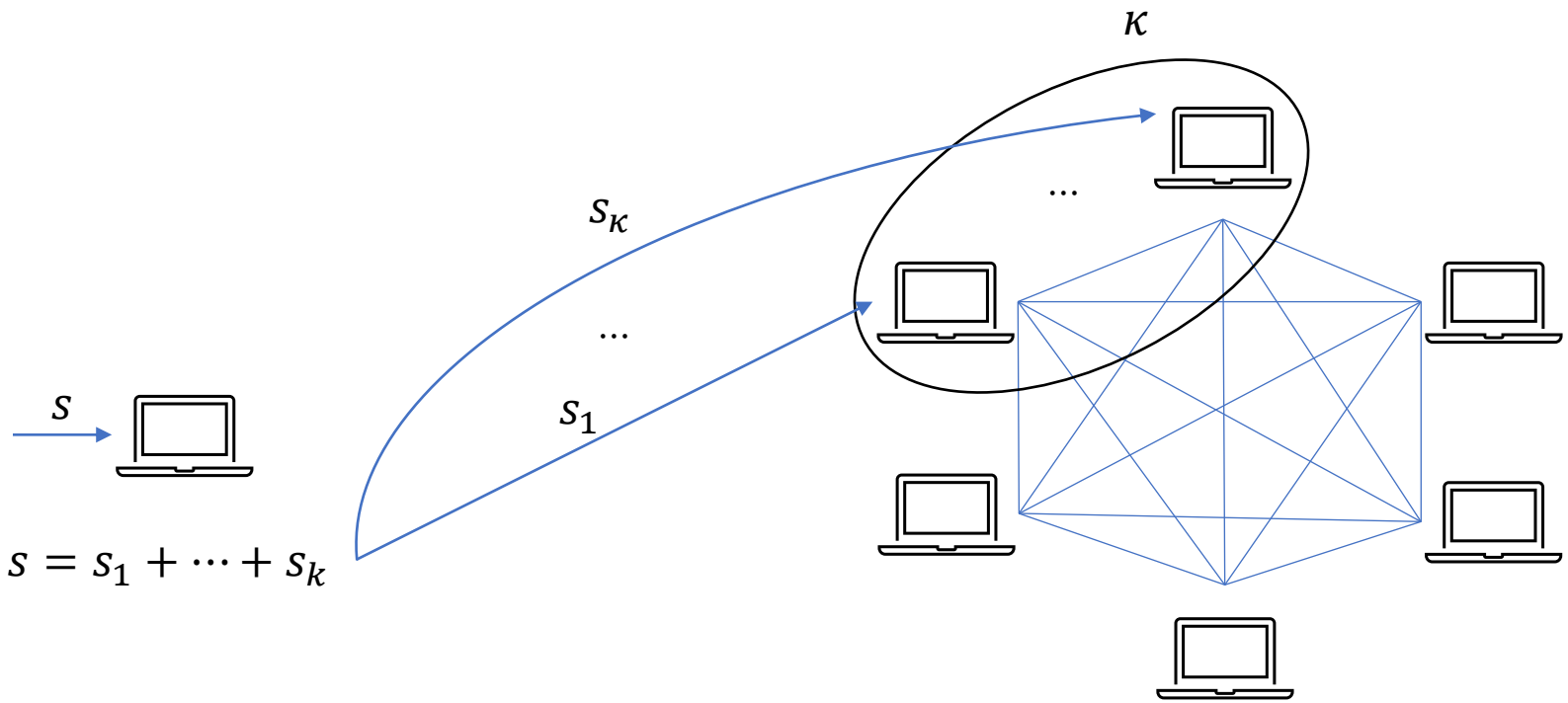
A Simple Example



$$s = s_1 + \cdots + s_k$$

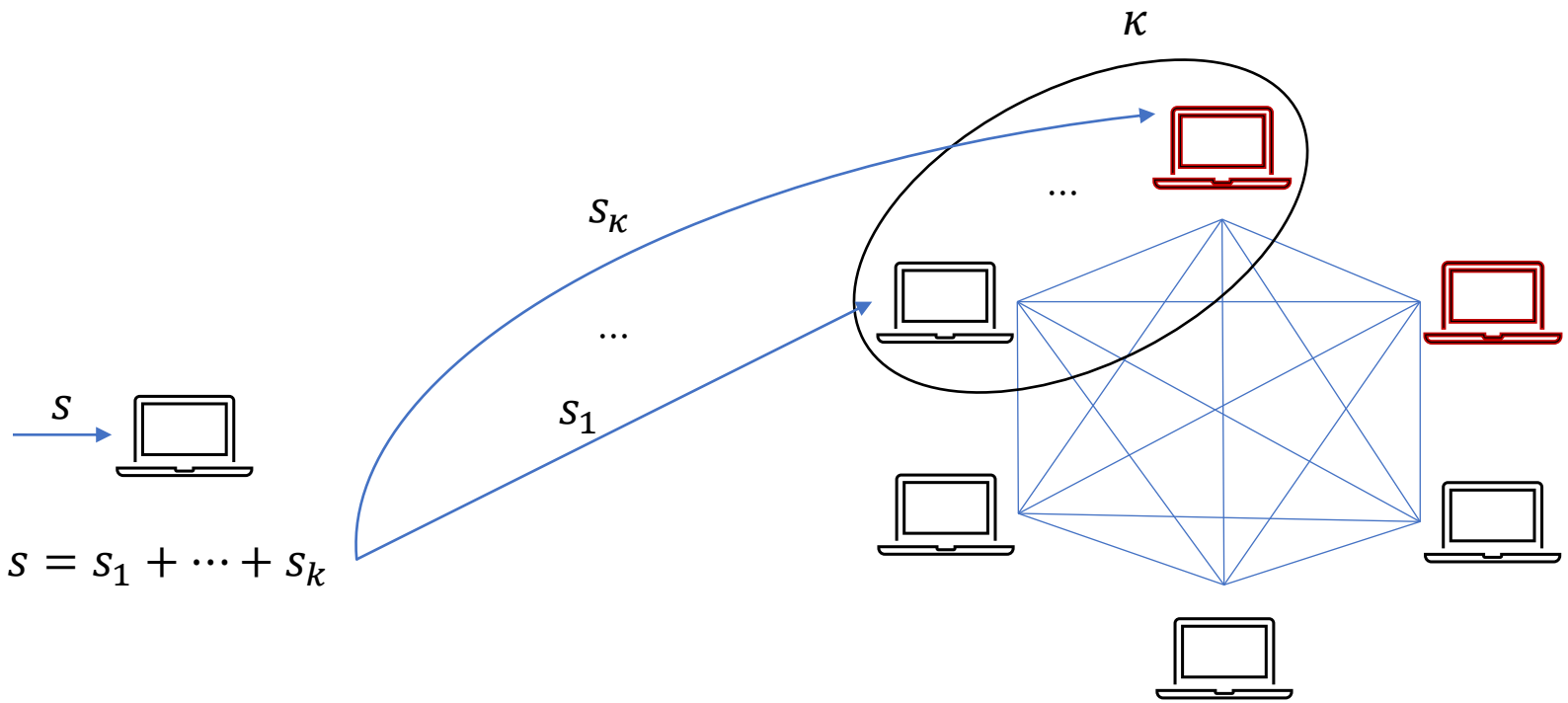


A Simple Example



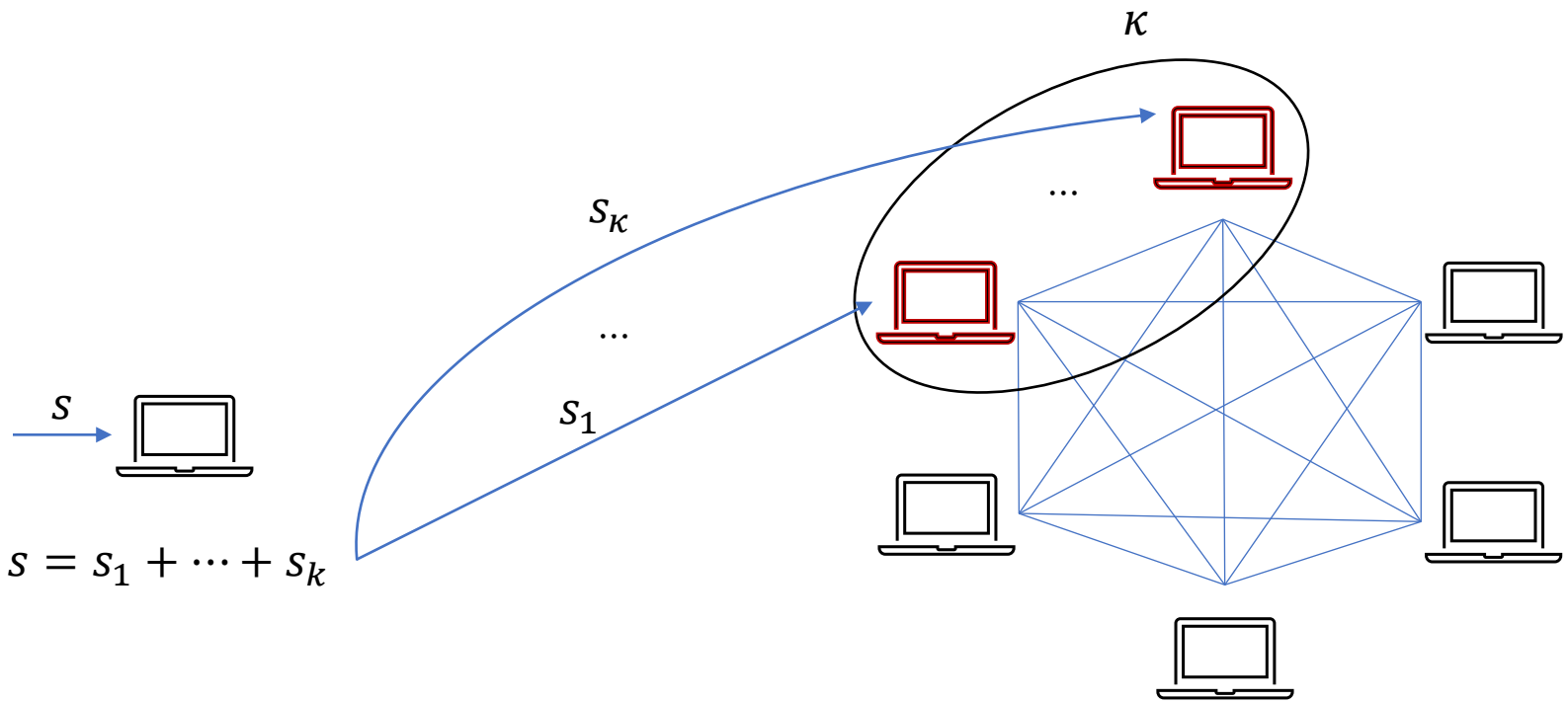
$s = s_1 + \cdots + s_k$

A Simple Example



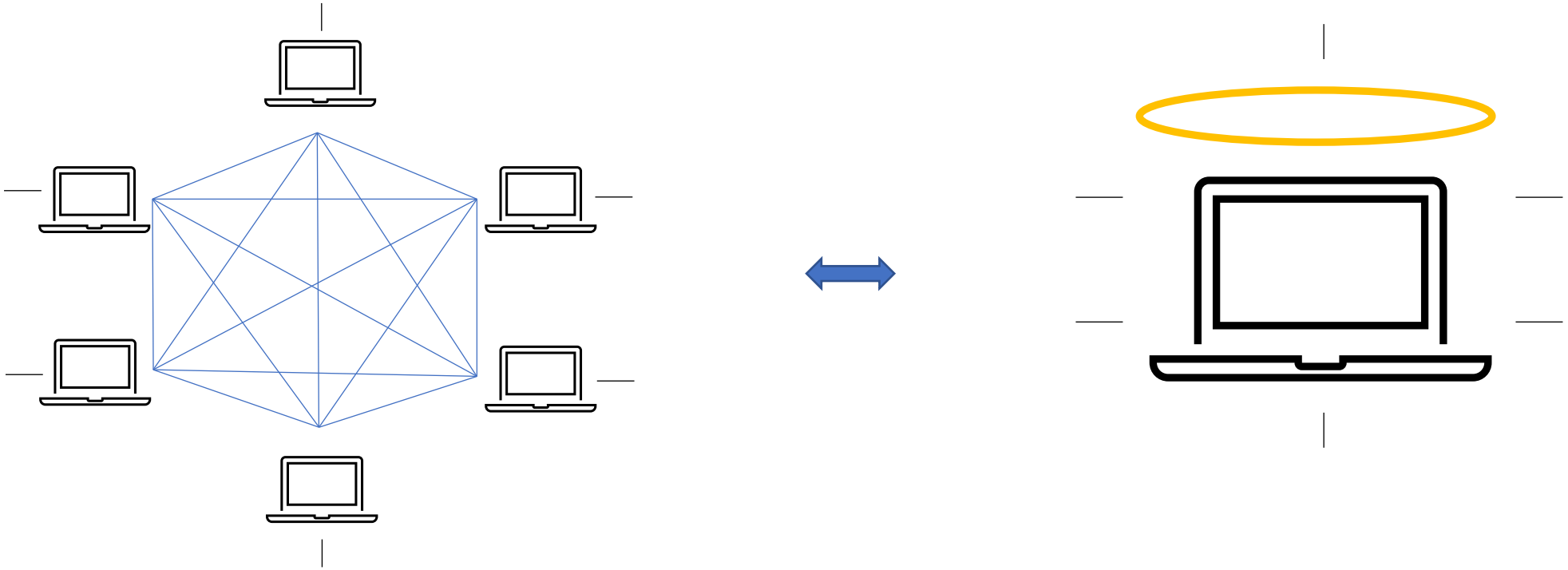
A static adversary corrupting κ parties only learns s with small probability

A Simple Example

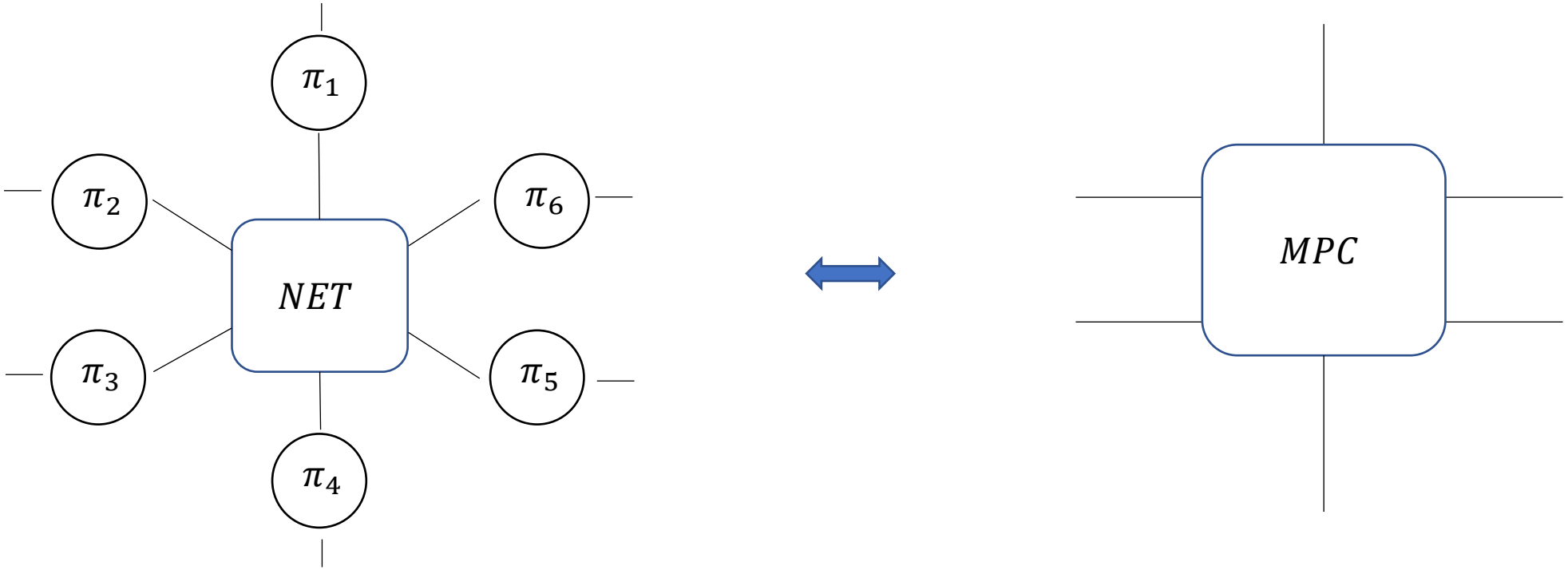


An adaptive adversary corrupting κ parties can always learn s

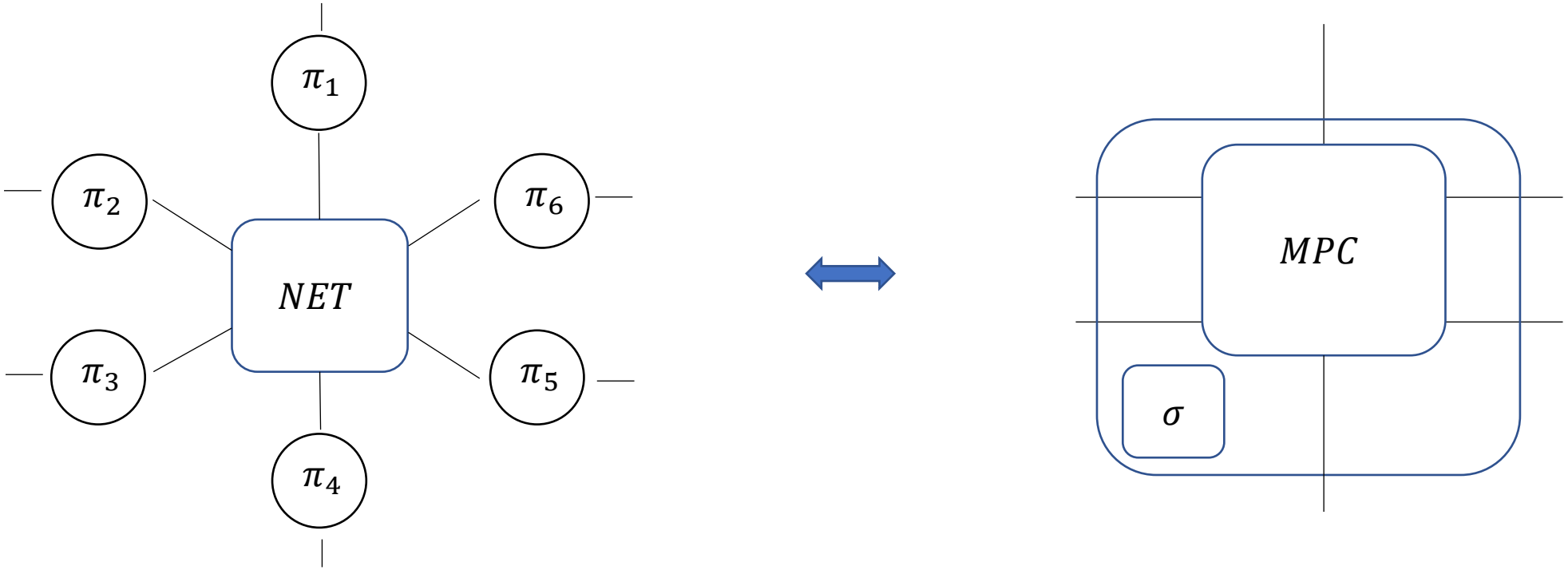
Standard Adaptive Security



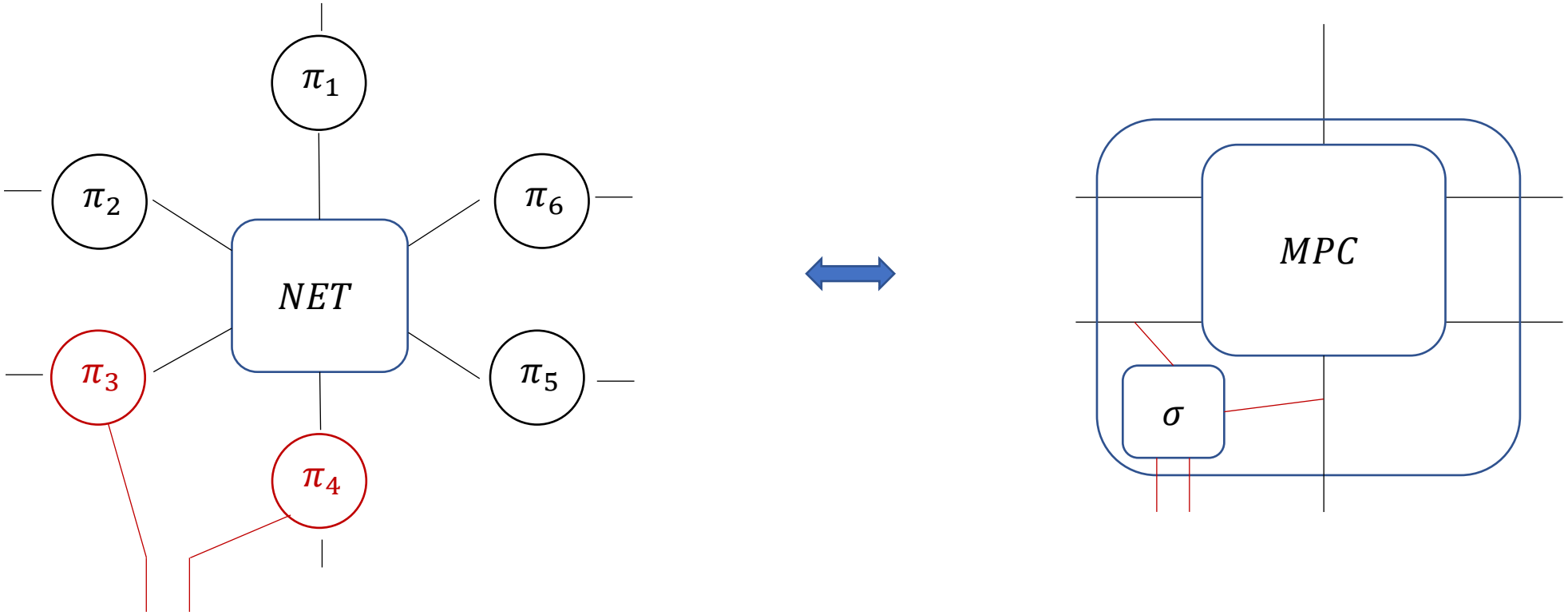
Standard Adaptive Security



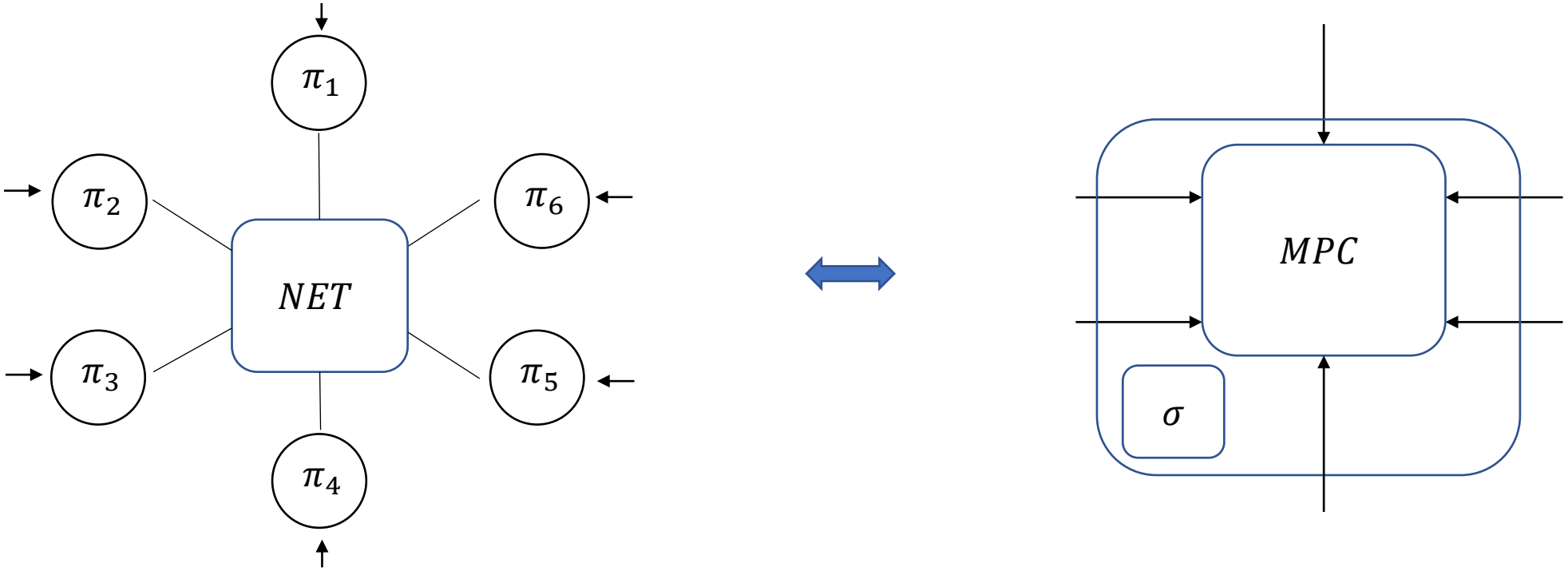
Standard Adaptive Security



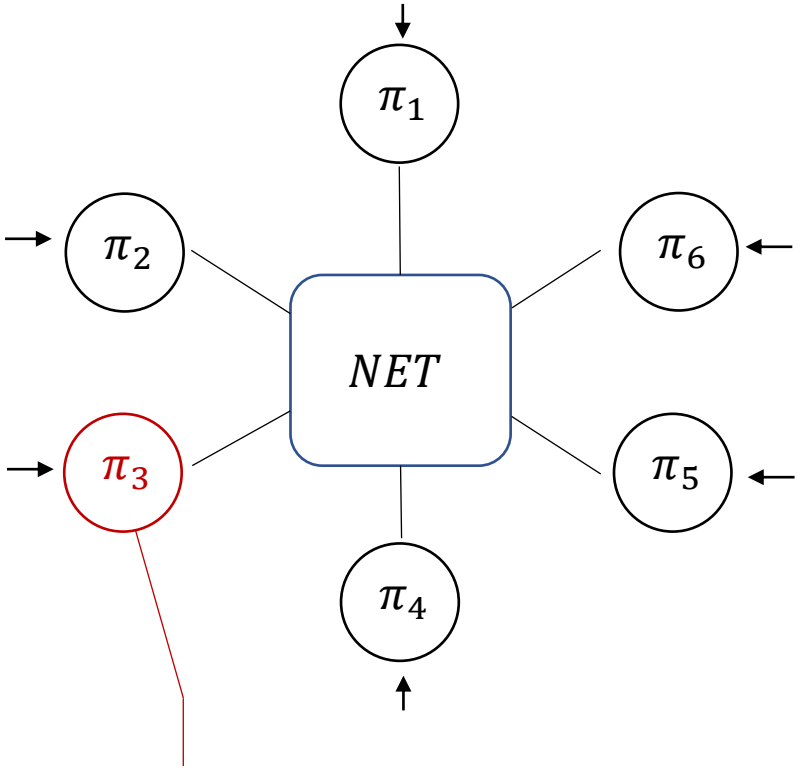
Standard Adaptive Security

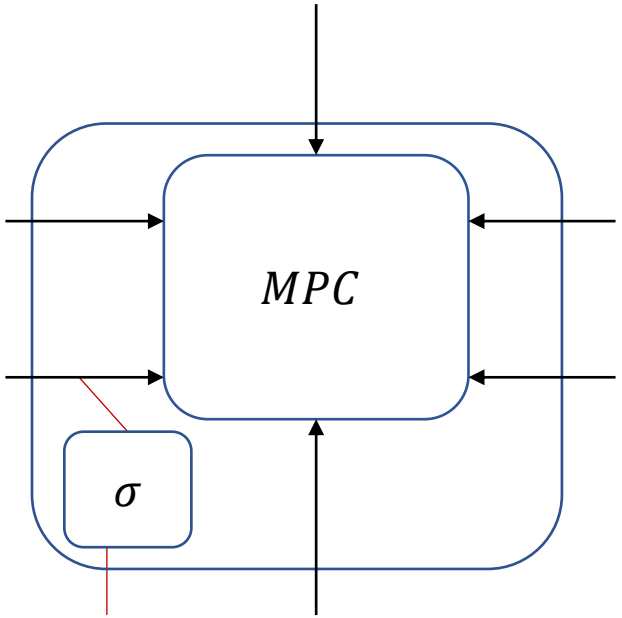


Standard Adaptive Security

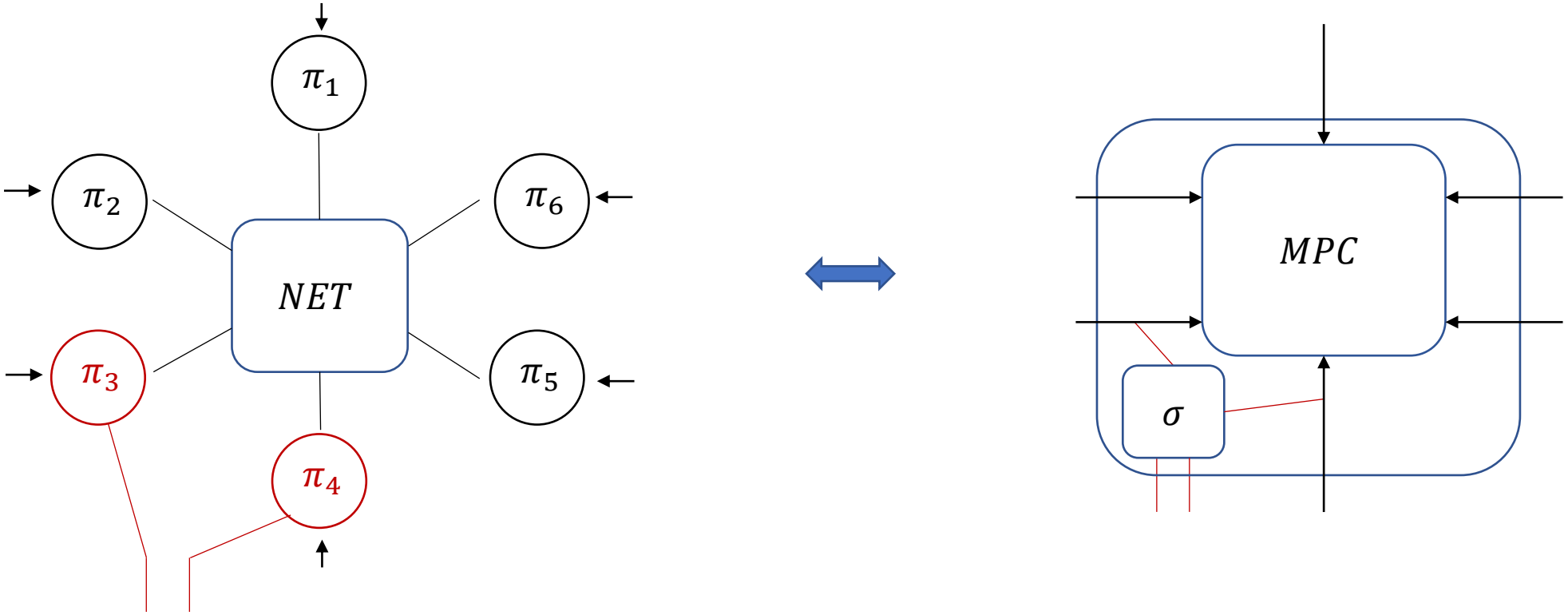


Standard Adaptive Security

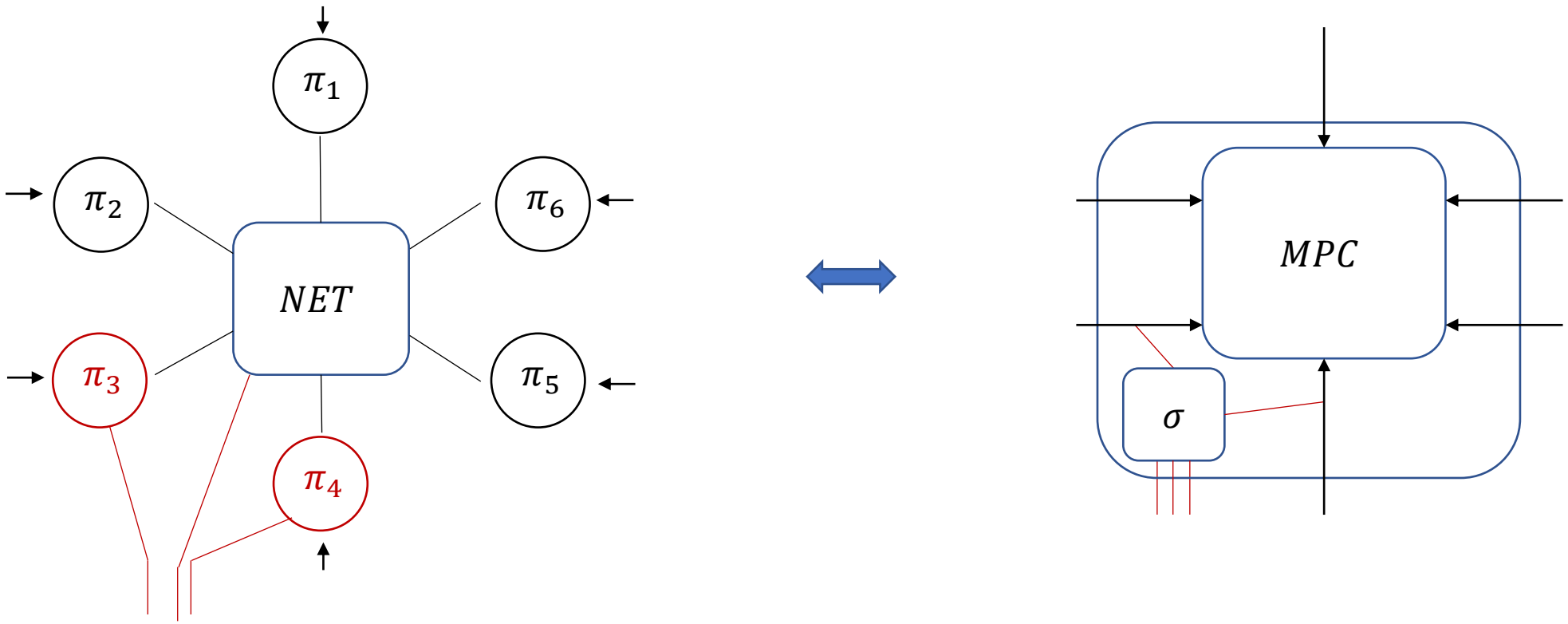




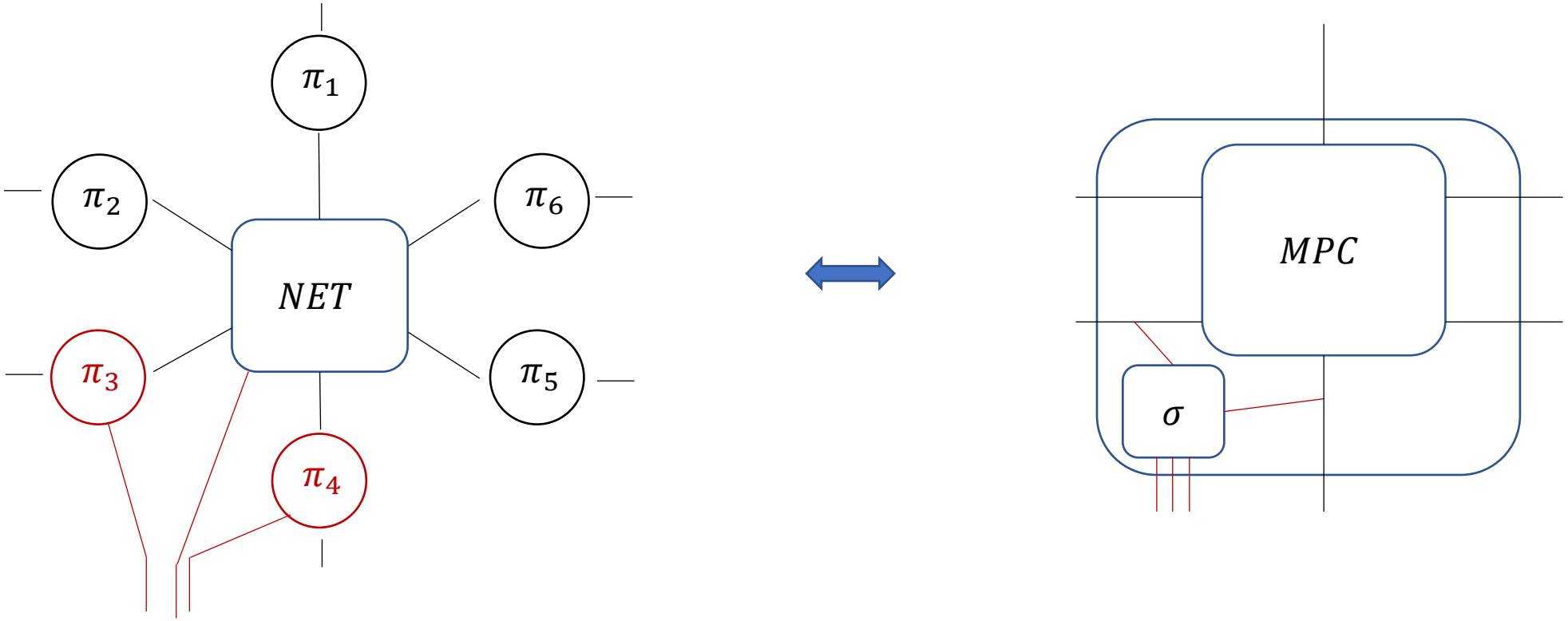
Standard Adaptive Security



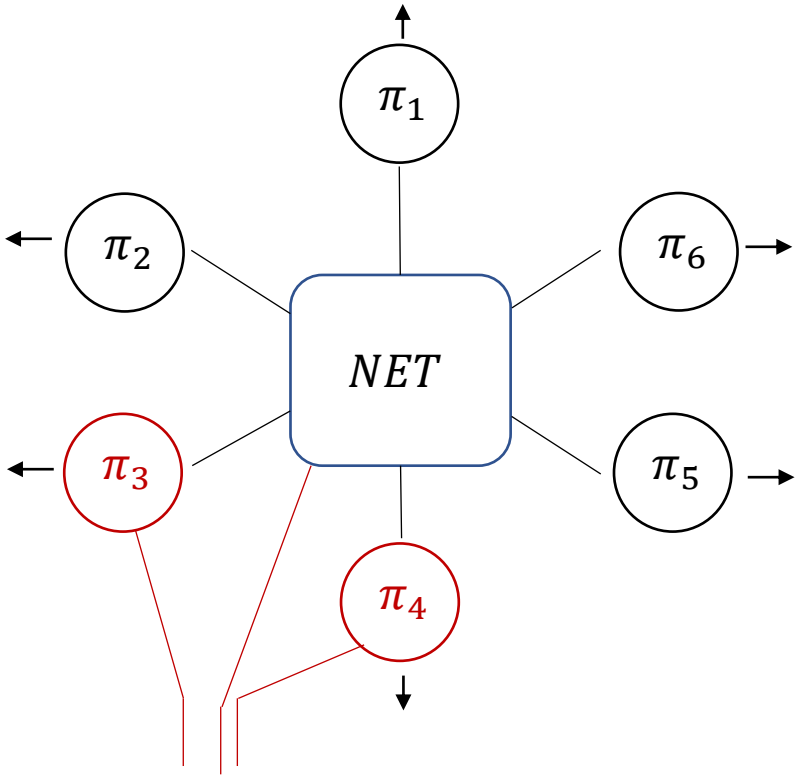
Standard Adaptive Security

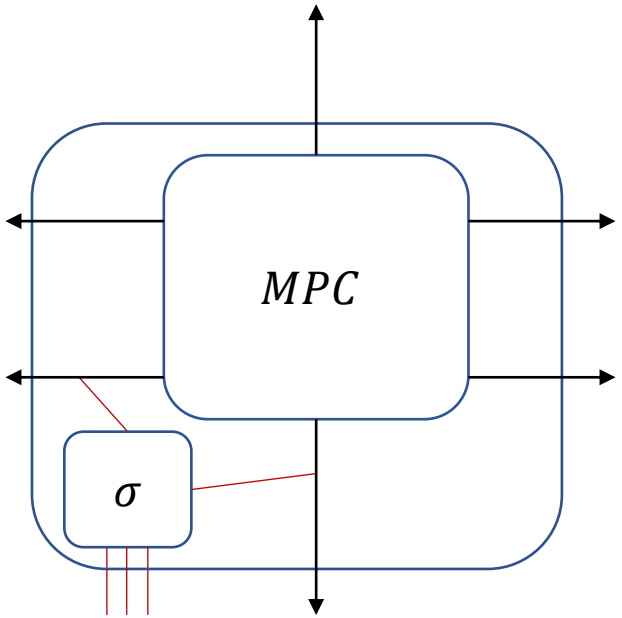


Standard Adaptive Security

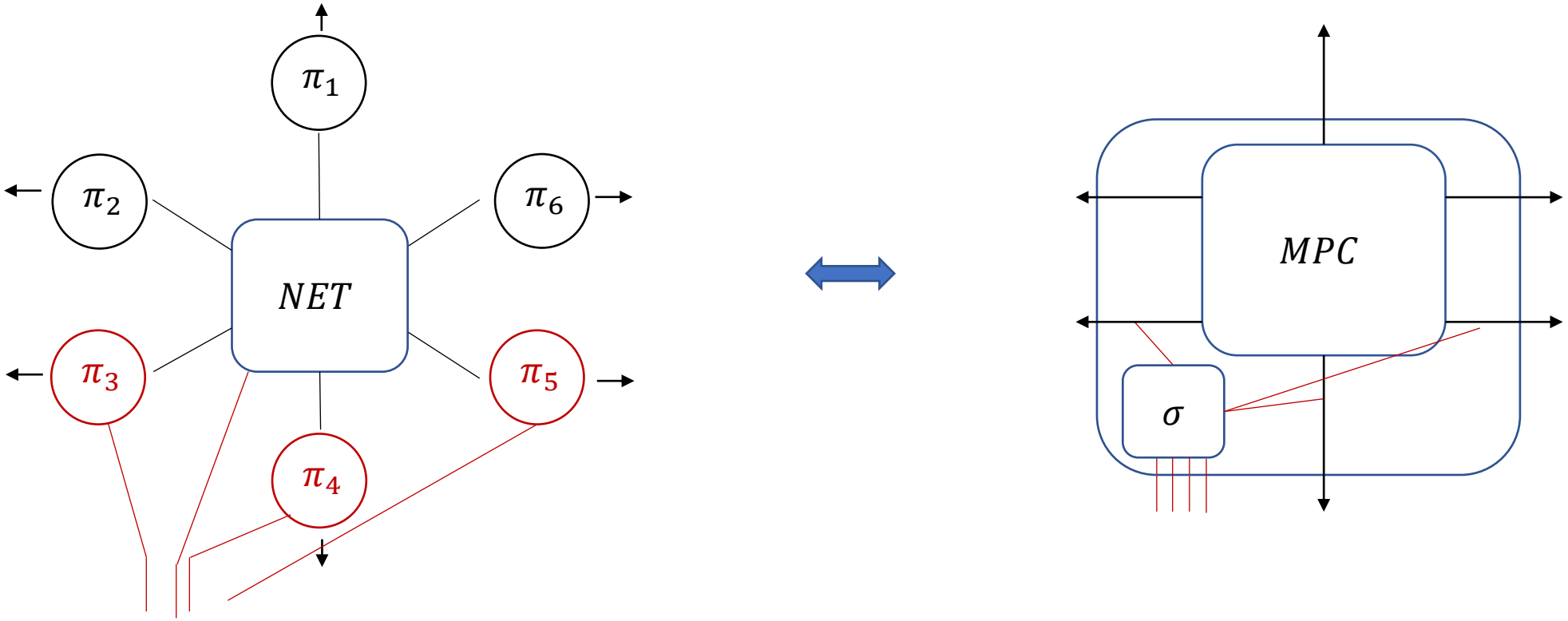


Standard Adaptive Security

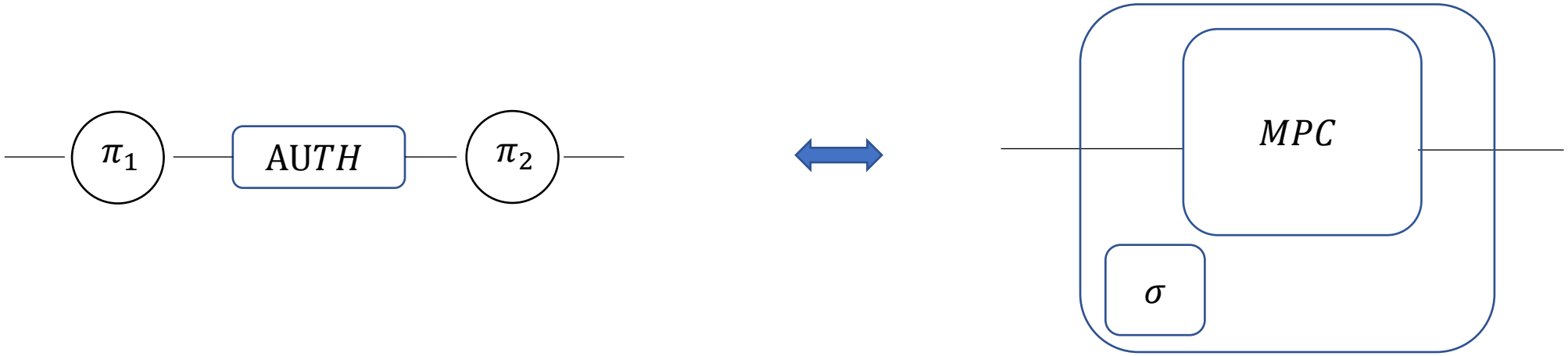




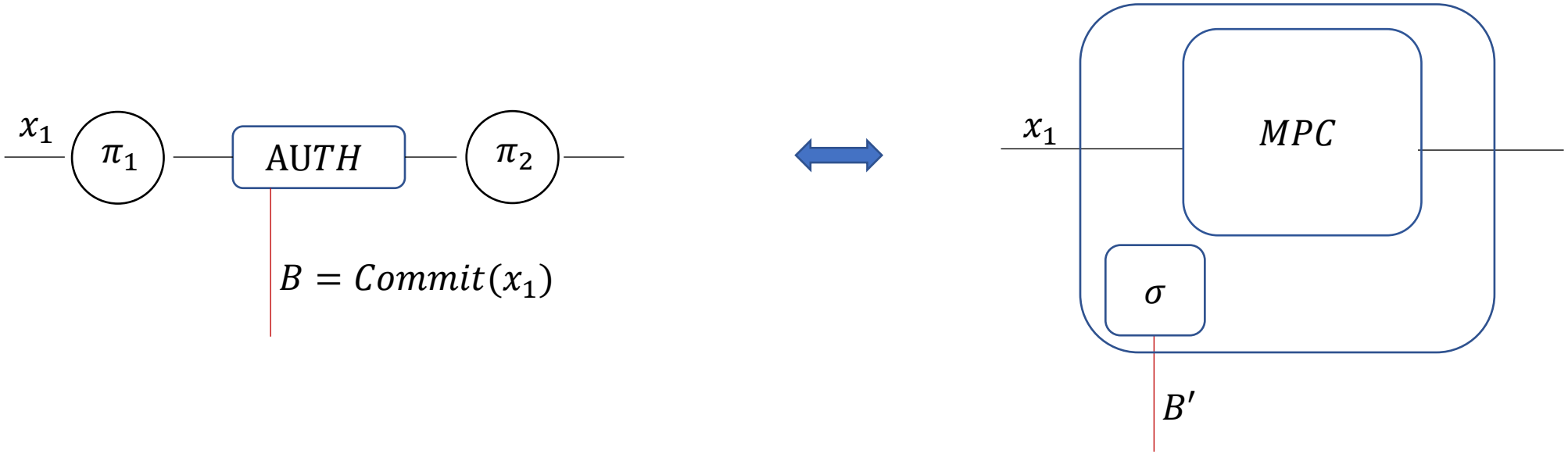
Standard Adaptive Security



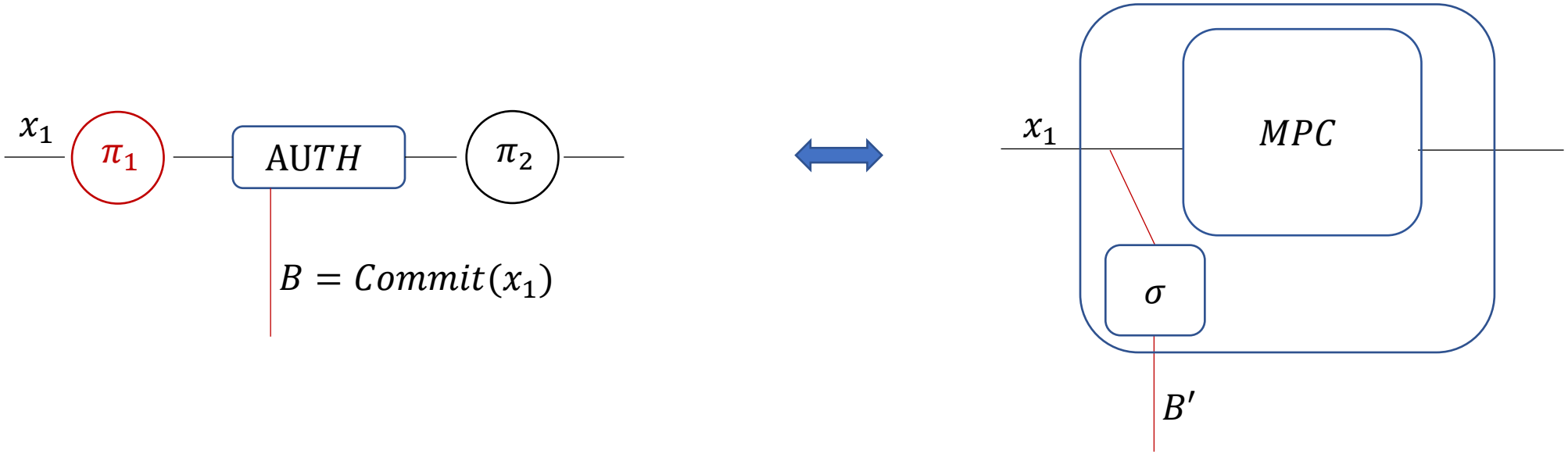
Commitment Problem



Commitment Problem



Commitment Problem



σ cannot open B' to x_1

Commitment Problem

Super-Secure Protocol

1. Receive input x_1
2.
3.
4.
…

Commitment Problem

Random Stuff

1. Receive input x_1
2. $B = Commit(x_1)$
3. Publish B

Super-Secure Protocol

1. Receive input x_1
2.
3.
4.
…

Commitment Problem

Random Stuff

1. Receive input x_1
2. $B = Commit(x_1)$
3. Publish B

Super-Secure Protocol

1. Receive input x_1
2.
3.
4.
…

Secure Erasures

Non-committing primitives

Is there a natural definition for adaptive security that is not subject to the commitment problem?

Our Solution

$\forall X \subseteq \mathcal{P}$ as long as X is honest: $Guarantee(X)$ holds

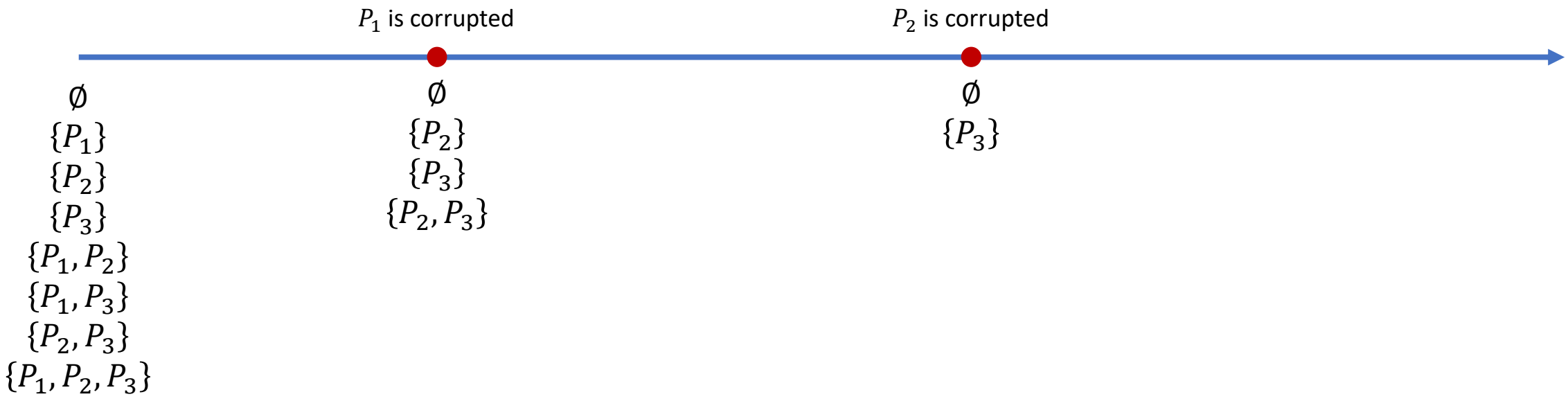
$\emptyset$
$\{P_1\}$
$\{P_2\}$
$\{P_3\}$
$\{P_1, P_2\}$
$\{P_1, P_3\}$
$\{P_2, P_3\}$
$\{P_1, P_2, P_3\}$

Our Solution

$\forall X \subseteq \mathcal{P}$ as long as X is honest: $Guarantee(X)$ holds

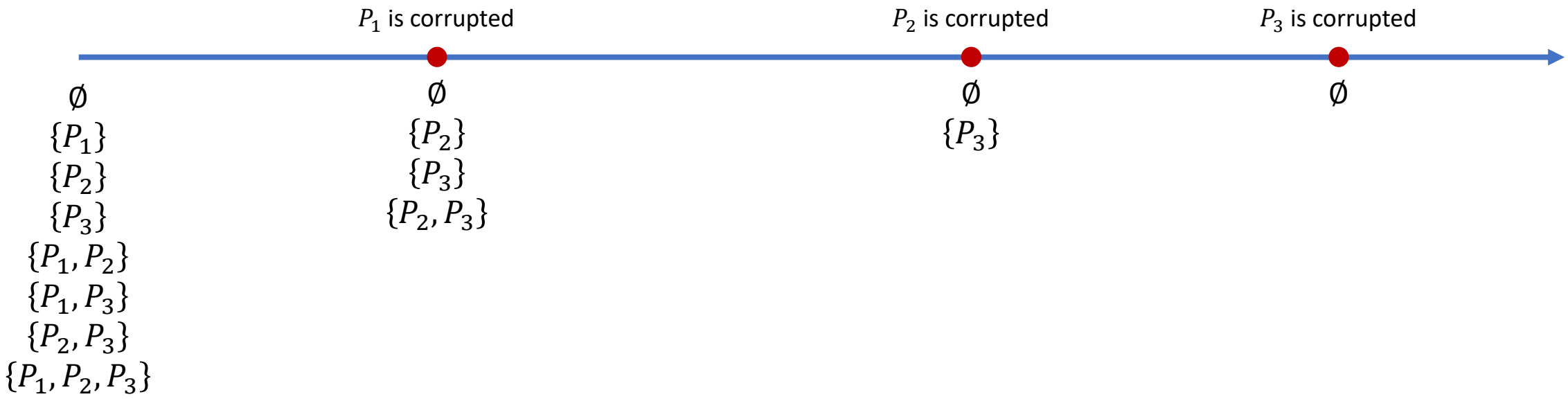
Our Solution

$\forall X \subseteq \mathcal{P}$ as long as X is honest: $Guarantee(X)$ holds



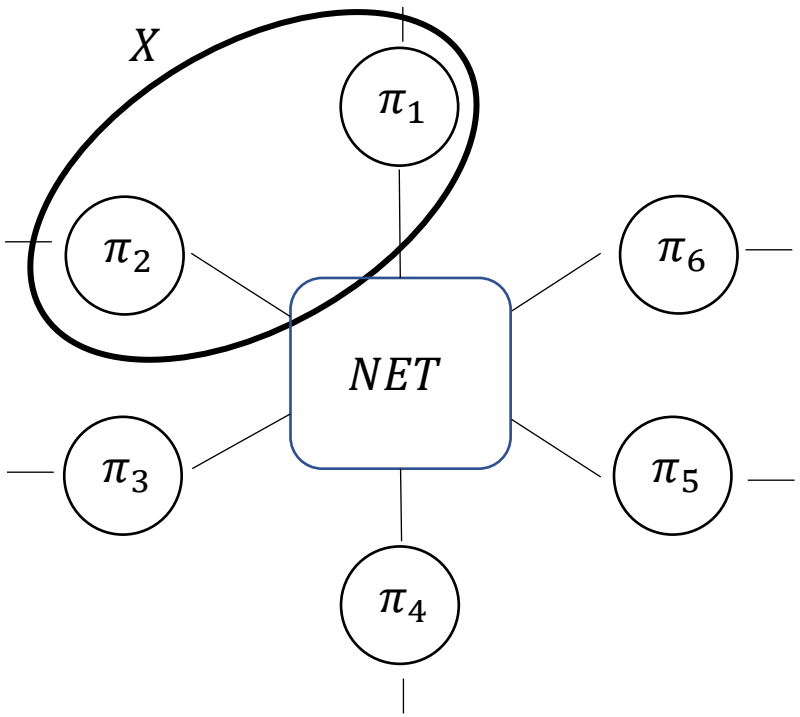
Our Solution

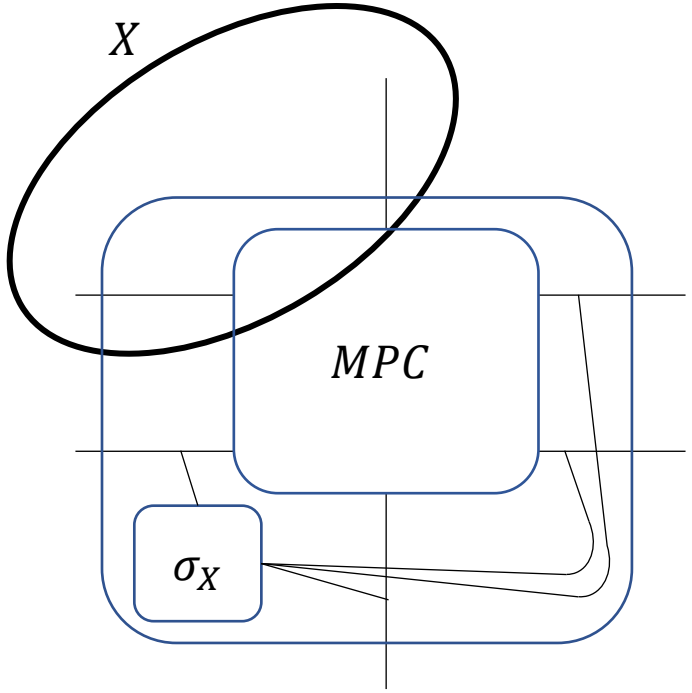
$\forall X \subseteq \mathcal{P}$ as long as X is honest: $Guarantee(X)$ holds



Our Solution

$Guarantee(X)$:

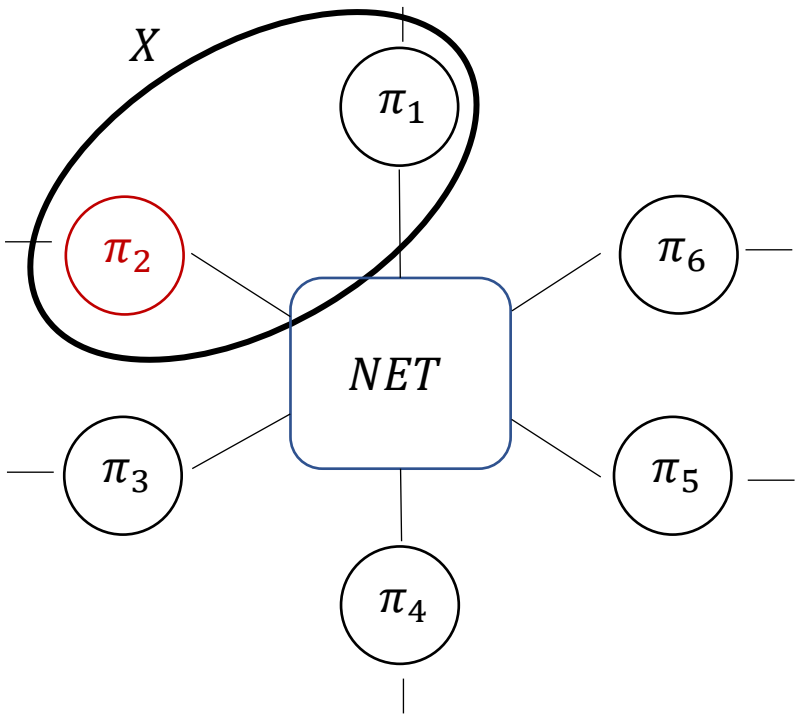


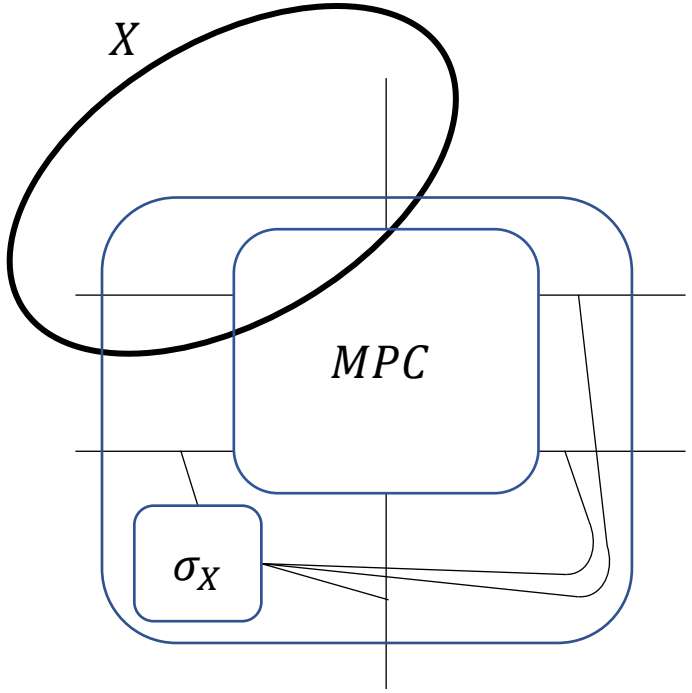


σ_X can read inputs from $\mathcal{P} \setminus X$

Our Solution

$Guarantee(X)$:



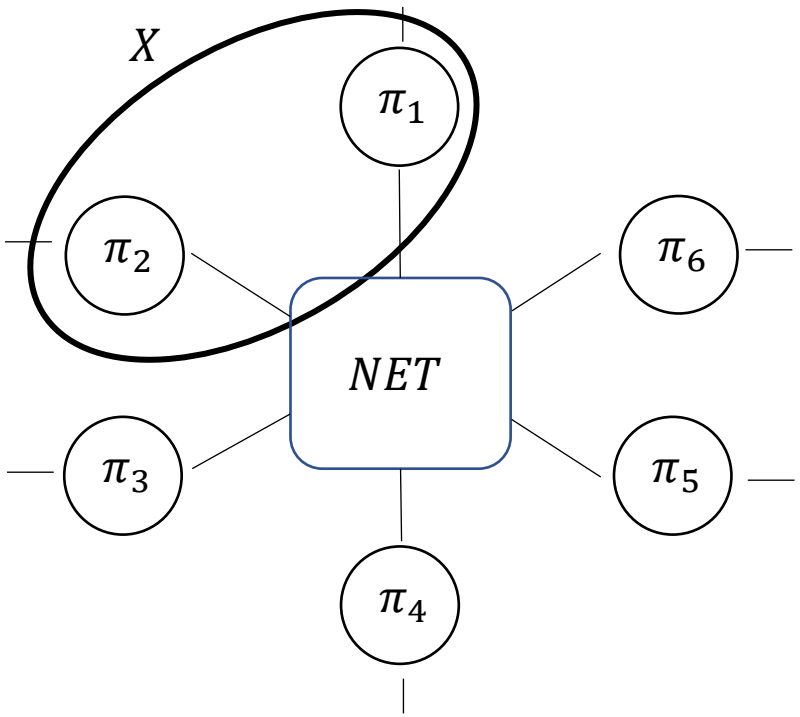


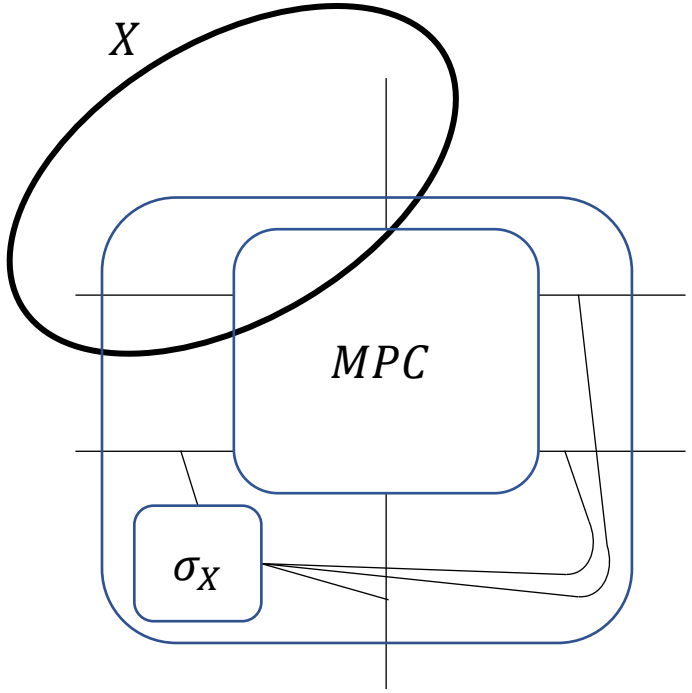
σ_X can read inputs from $\mathcal{P} \setminus X$

If any party in X is corrupted, the guarantee is dropped

Our Solution

$Guarantee(X)$:

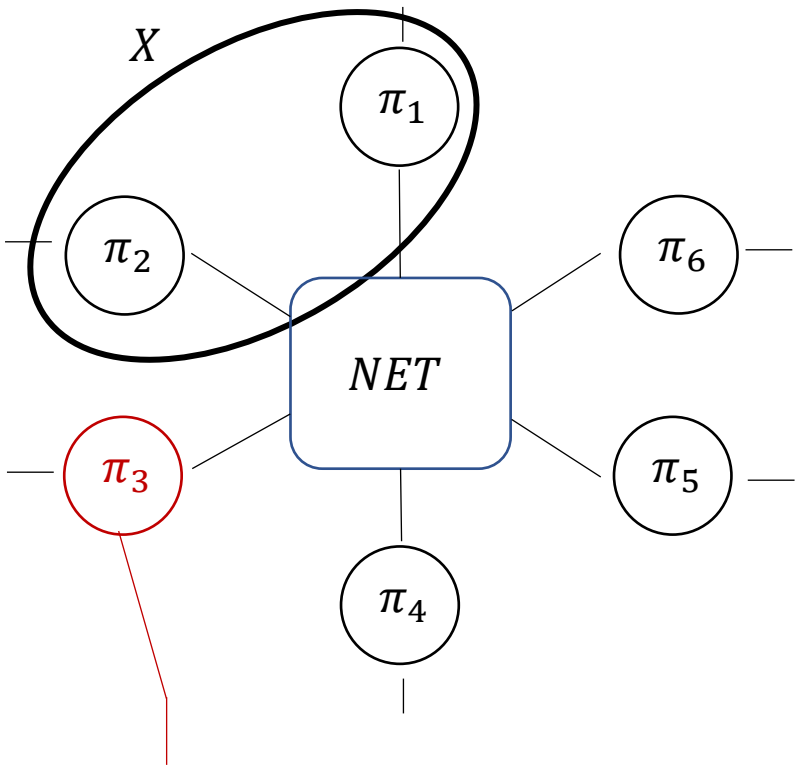


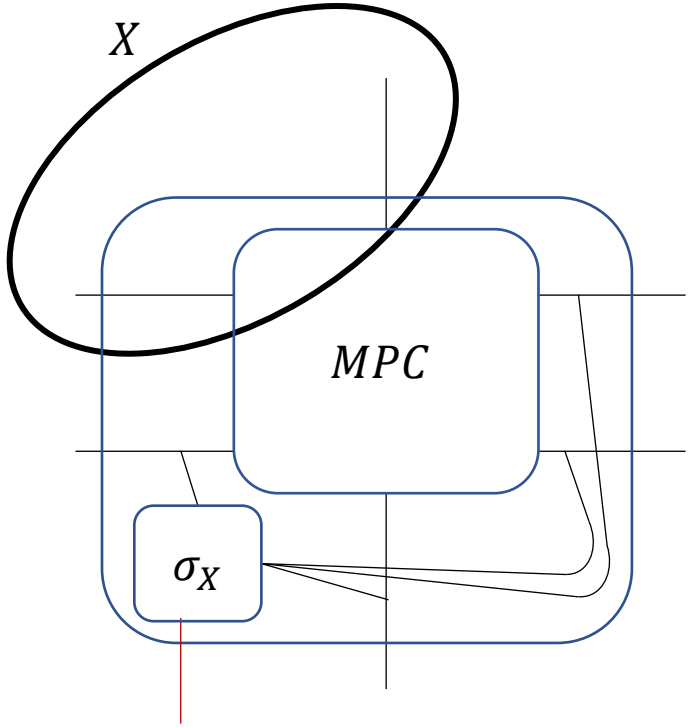


σ_X can read inputs from $\mathcal{P} \setminus X$

Our Solution

$Guarantee(X)$:

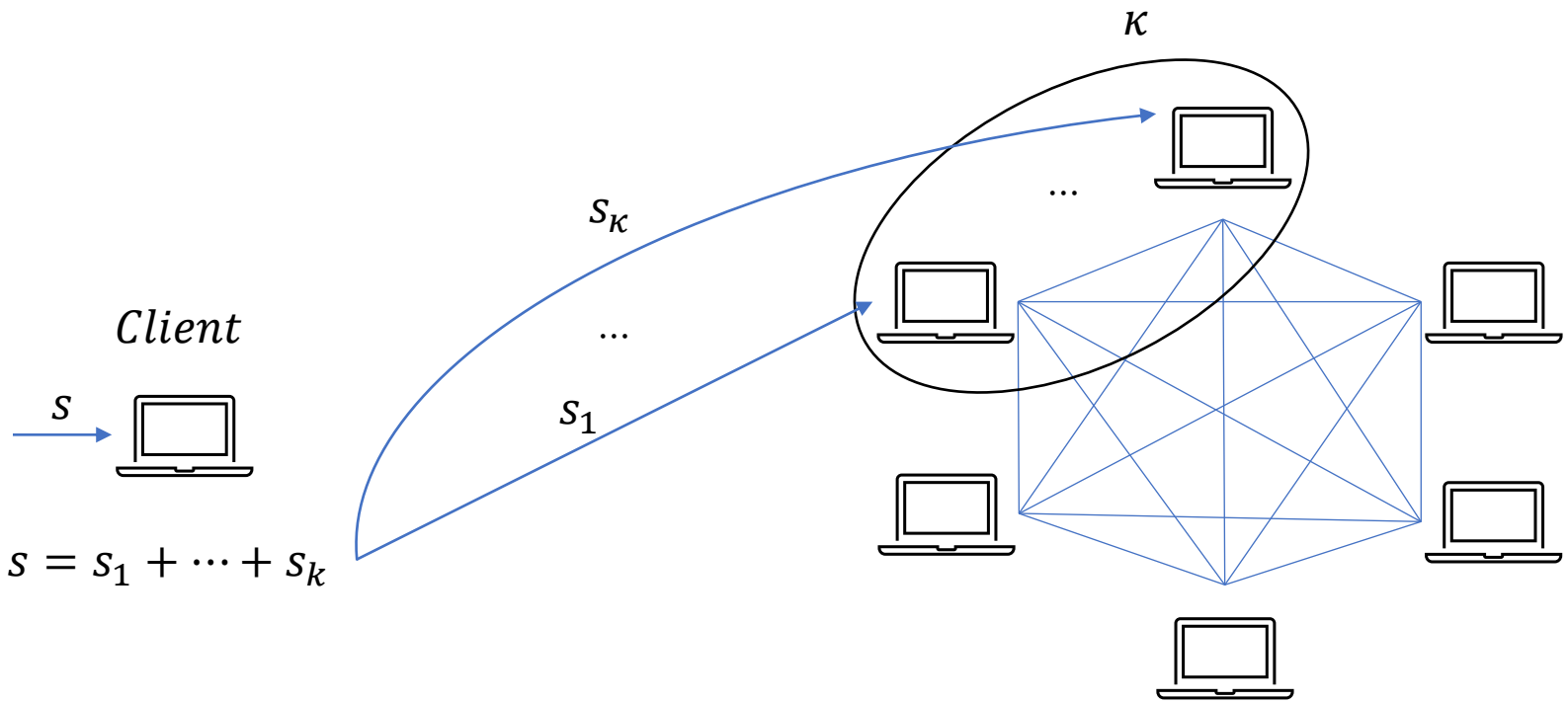




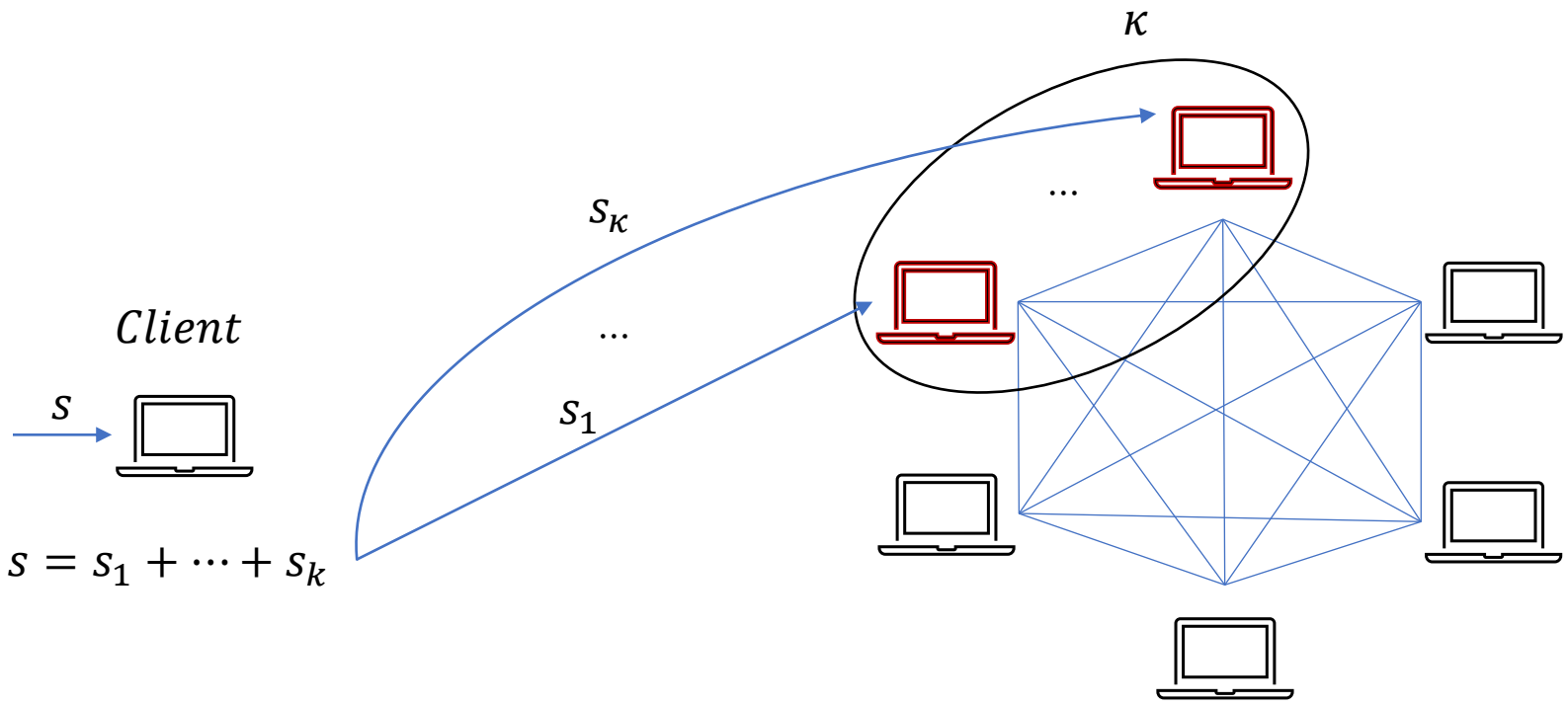
σ_X can read inputs from $\mathcal{P} \setminus X$

σ_X can explain the state of parties in $\mathcal{P} \setminus X$

A Simple Example



A Simple Example



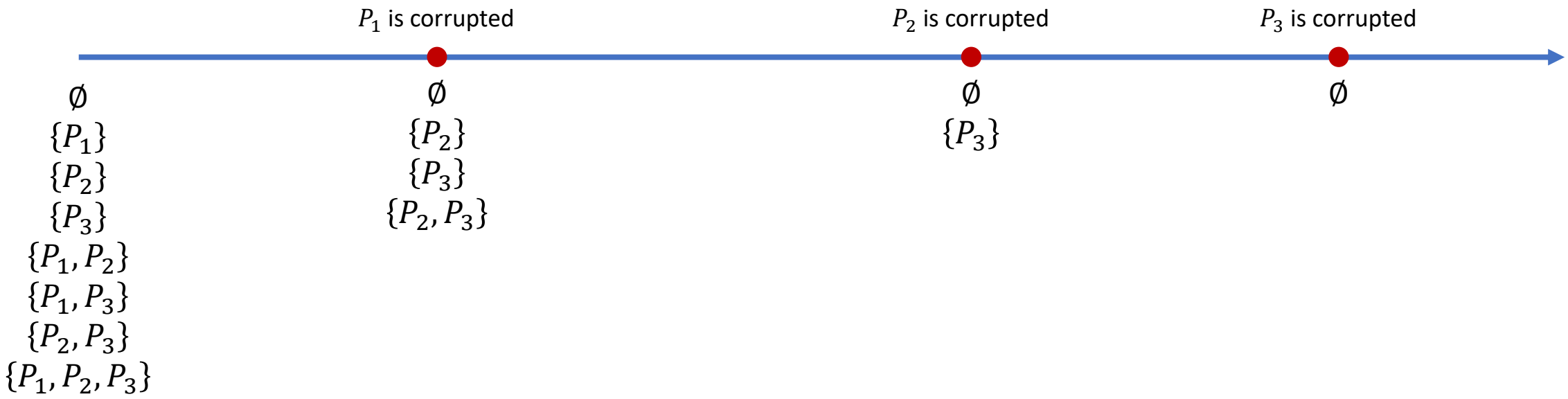
$X = \{Client\}$

$Guarantee(X)$ holds as long as $Client$ is honest

The adversary can adaptively corrupt the small set and learn the secret, which the simulator cannot output

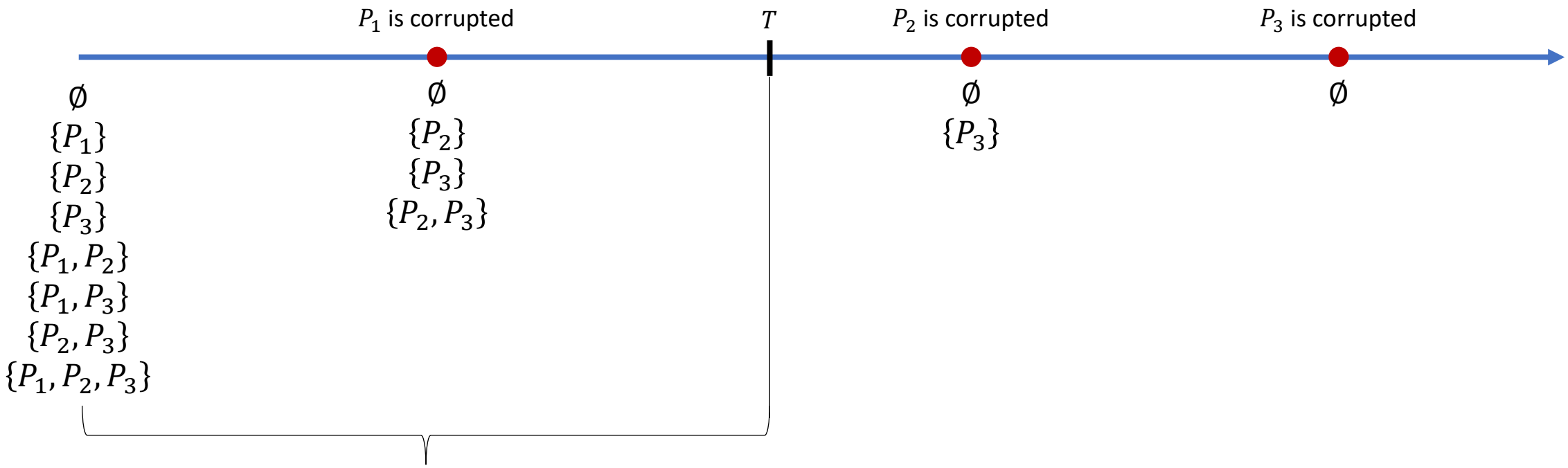
Our Solution

$\forall X \subseteq \mathcal{P}$ as long as X is honest: $Guarantee(X)$ holds



Our Solution

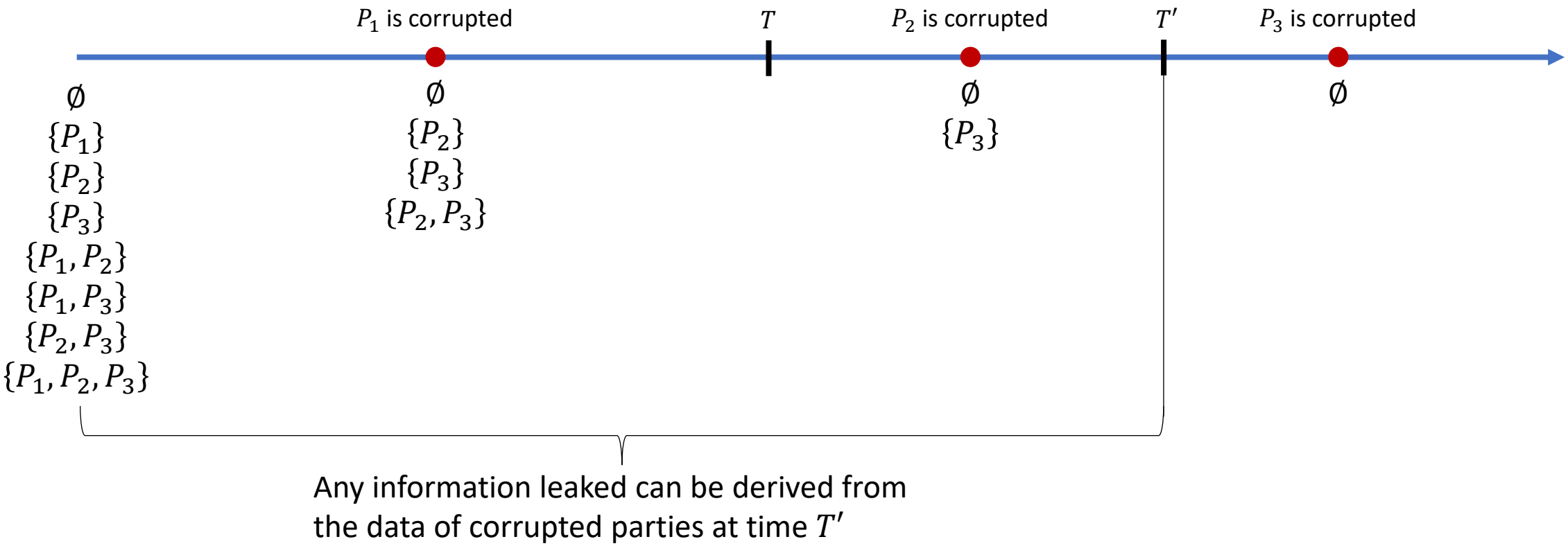
$\forall X \subseteq \mathcal{P}$ as long as X is honest: $Guarantee(X)$ holds



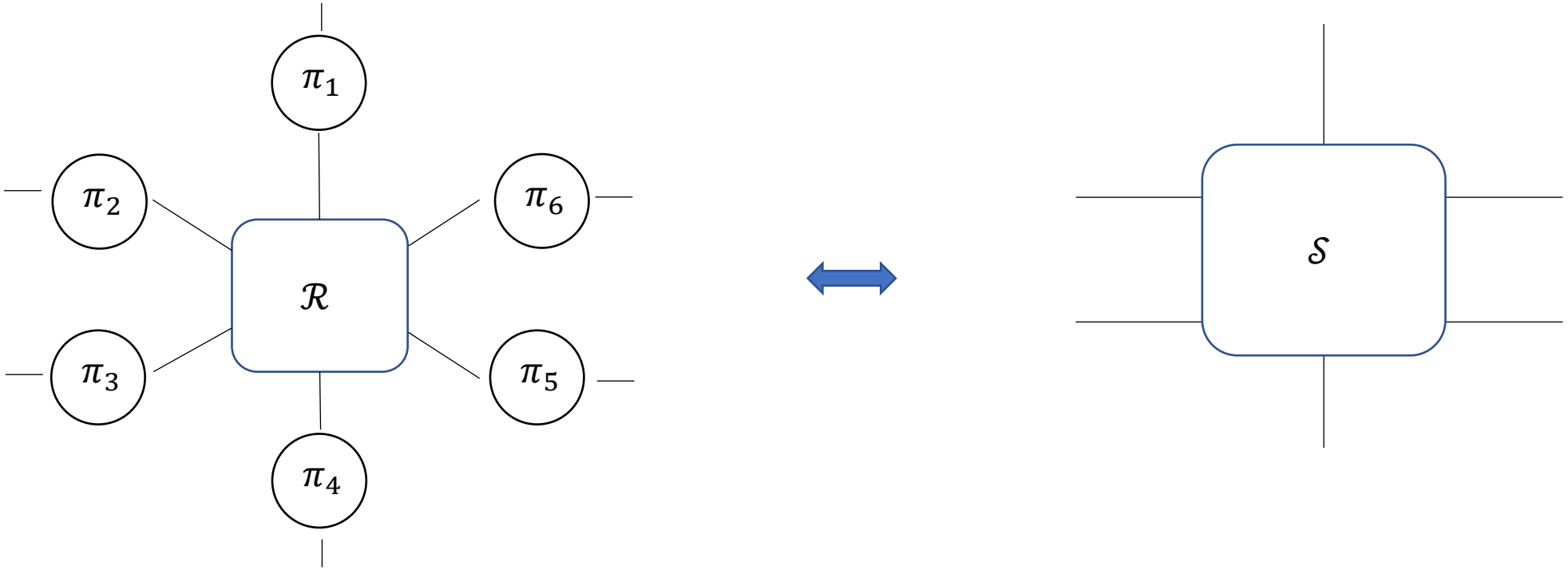
Any information leaked can be derived from the data of corrupted parties at time T

Our Solution

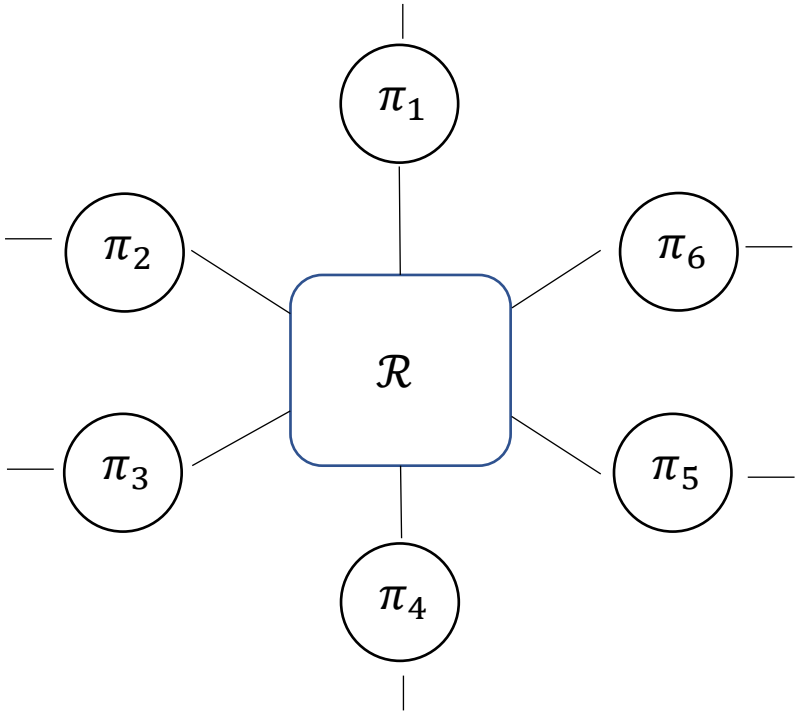
$\forall X \subseteq \mathcal{P}$ as long as X is honest: $Guarantee(X)$ holds



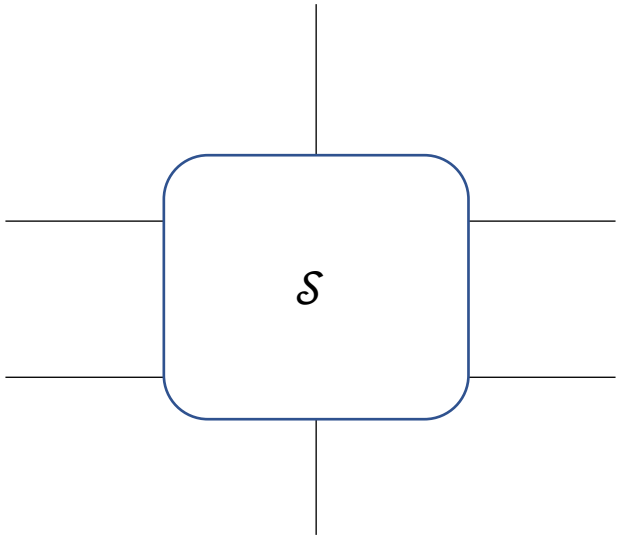
Constructive Cryptography



Constructive Cryptography



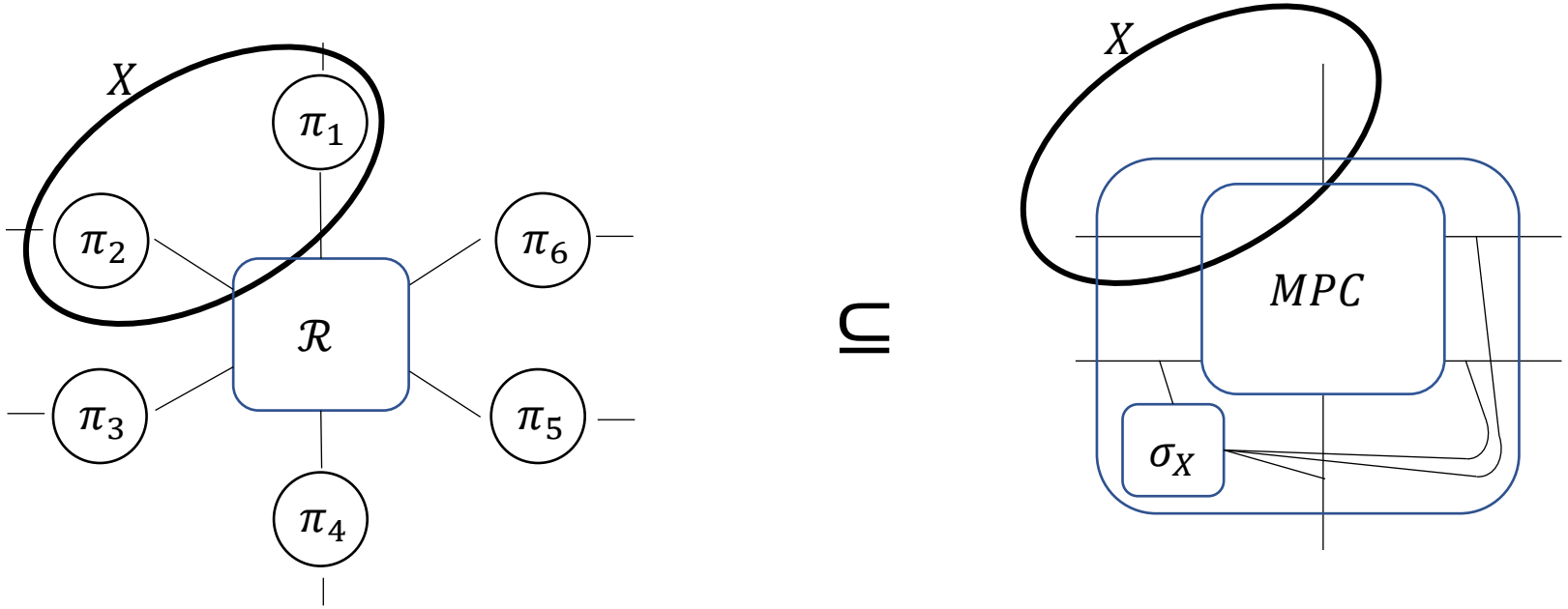
$\subseteq$



$$\pi\mathcal{R} \subseteq \mathcal{S}$$

Constructive Cryptography

$Guarantee(X)$ holds until any party in X is corrupted



$$\forall X \subseteq \mathcal{P}\colon \pi\mathcal{R} \subseteq \mathcal{S}_X \coloneqq (\sigma_X MPC)^{\mathcal{E}_X}$$

$$\Leftrightarrow \pi\mathcal{R} \subseteq \mathcal{S} \coloneqq \bigcap_{X \subseteq \mathcal{P}} \mathcal{S}_X$$

Set of all systems that behave like $\sigma_X MPC$
until event $\mathcal{E}_X$ happens (any party in X is corrupted)

Some Lemmas

Standard Adaptive $\rightleftarrows$ New Notion $\rightleftarrows$ Static

New notion overcomes the commitment problem

Many protocols ‘believed’ to be adaptively secure in practice but not secure under current adaptive security notion satisfy the new notion: CDN, CLOS

Strong adaptive security guarantees

Typical examples separating static from adaptive security also separate static from the new notion

Contact info:
chendaliu@gmail.com
sites.google.com/view/chendaliu

Paper:
eprint.iacr.org/2021/1175