Multi-Party Computation in Presence of Corrupted Majorities

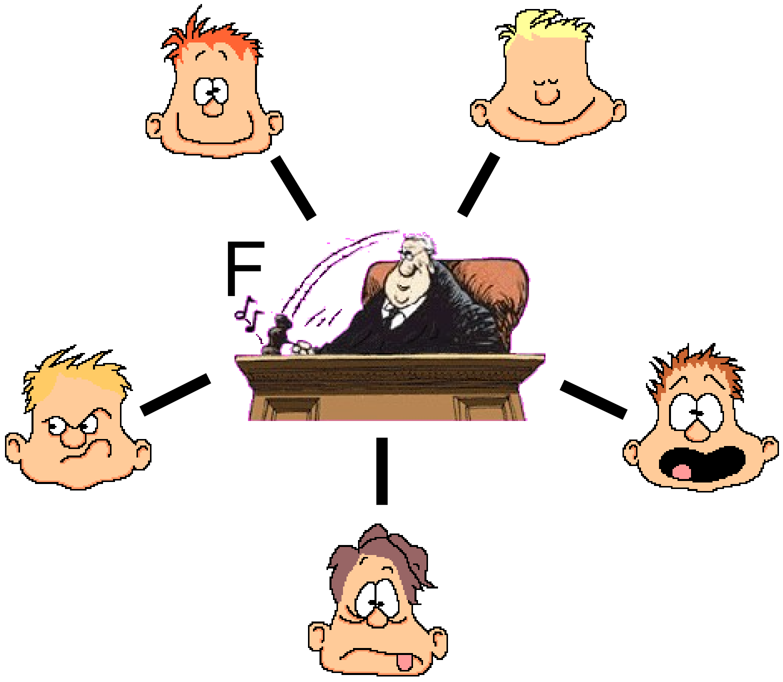
Dominik Raub

Institute of Theoretical Computer Science
ETH Zürich

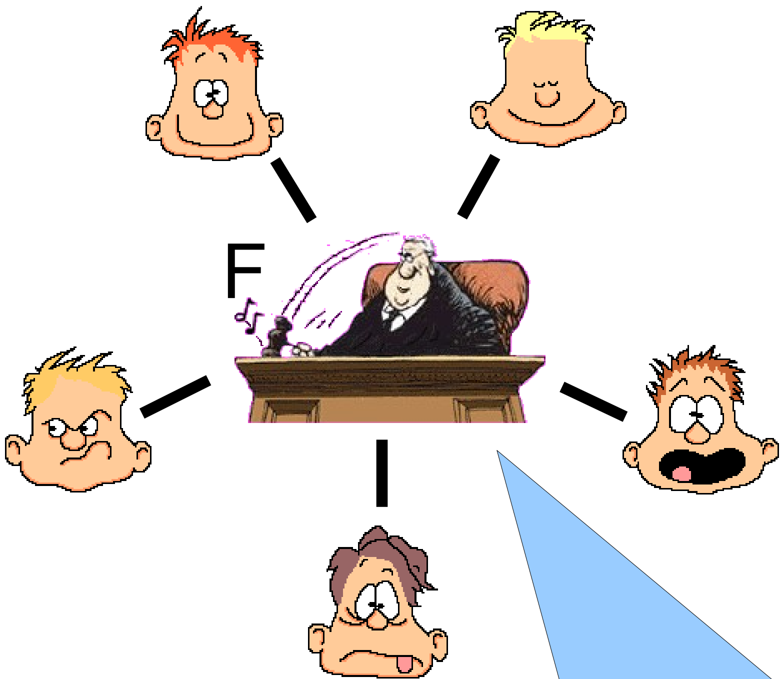
on joint work with
R. Künzler, J. Müller-Quade, C. Lucas, U. Maurer, M. Fitzi

Mäetaguse, 2009/10/04

Multi-Party Computation (MPC)



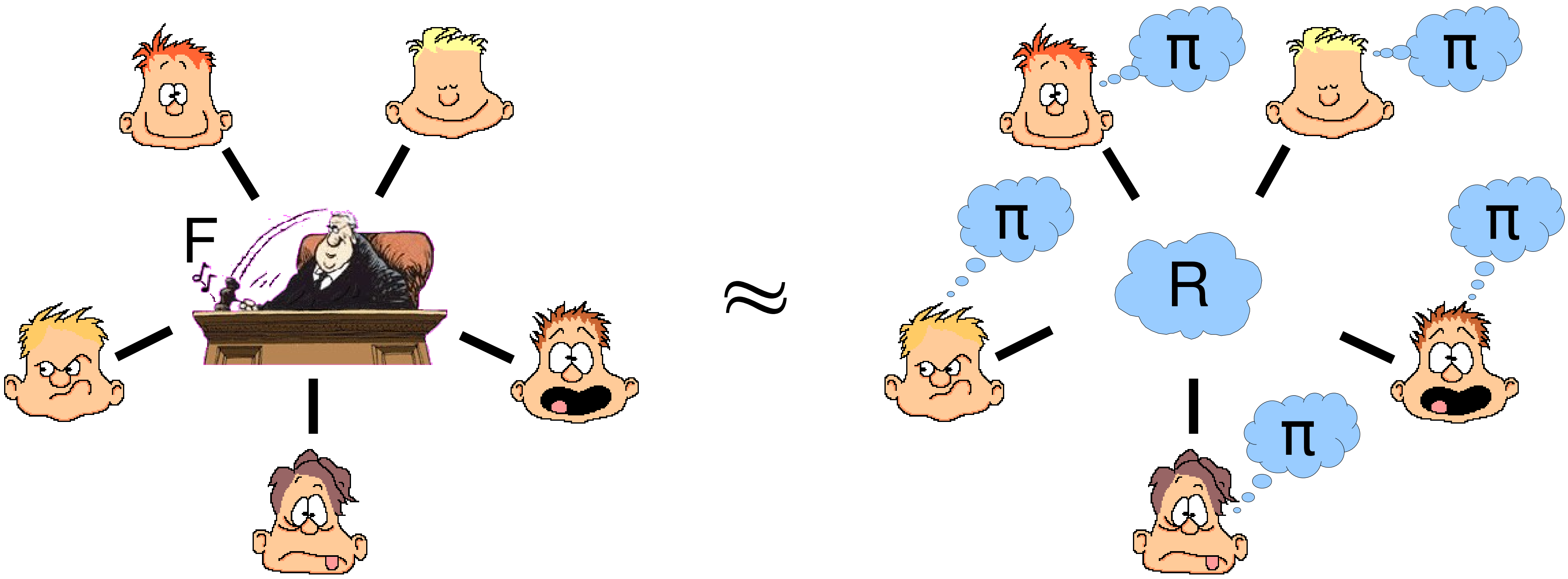
Multi-Party Computation (MPC)



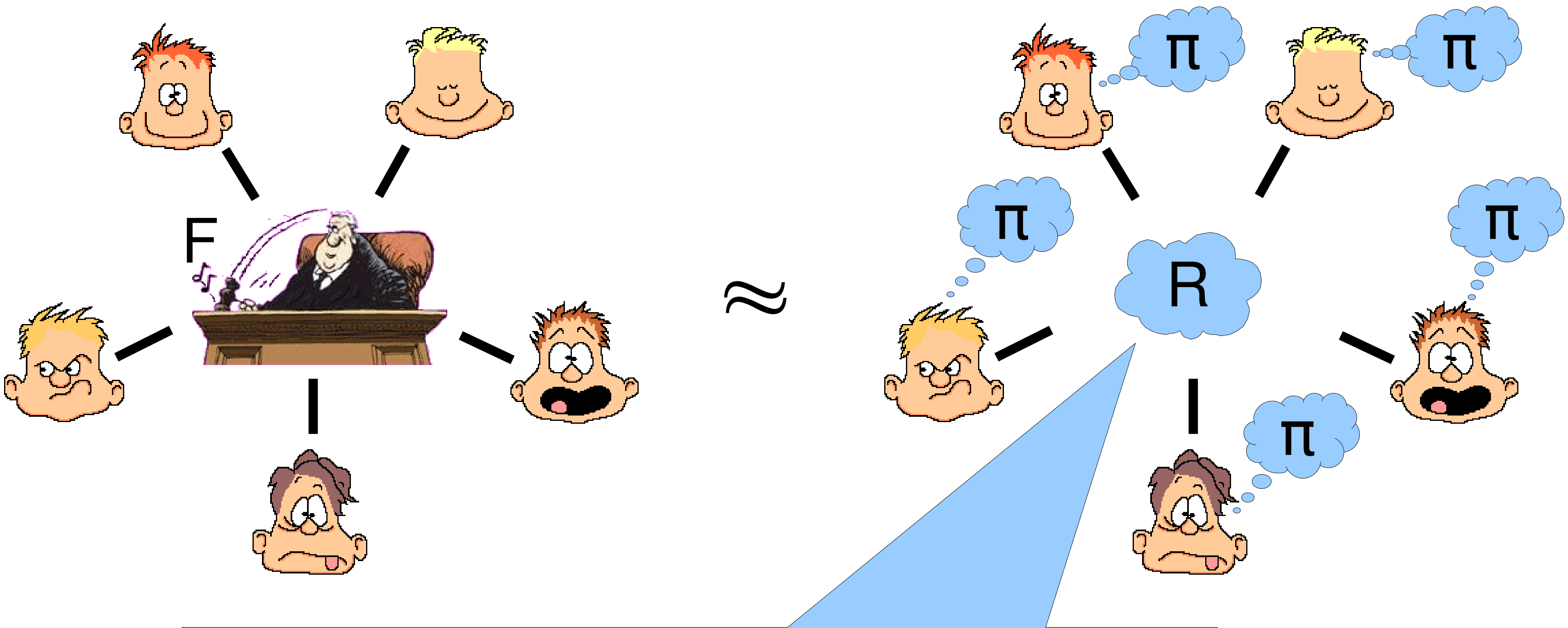
- Voting
- Auctions
- Who is richest?

⇒ privacy, correctness required

Multi-Party Computation (MPC)



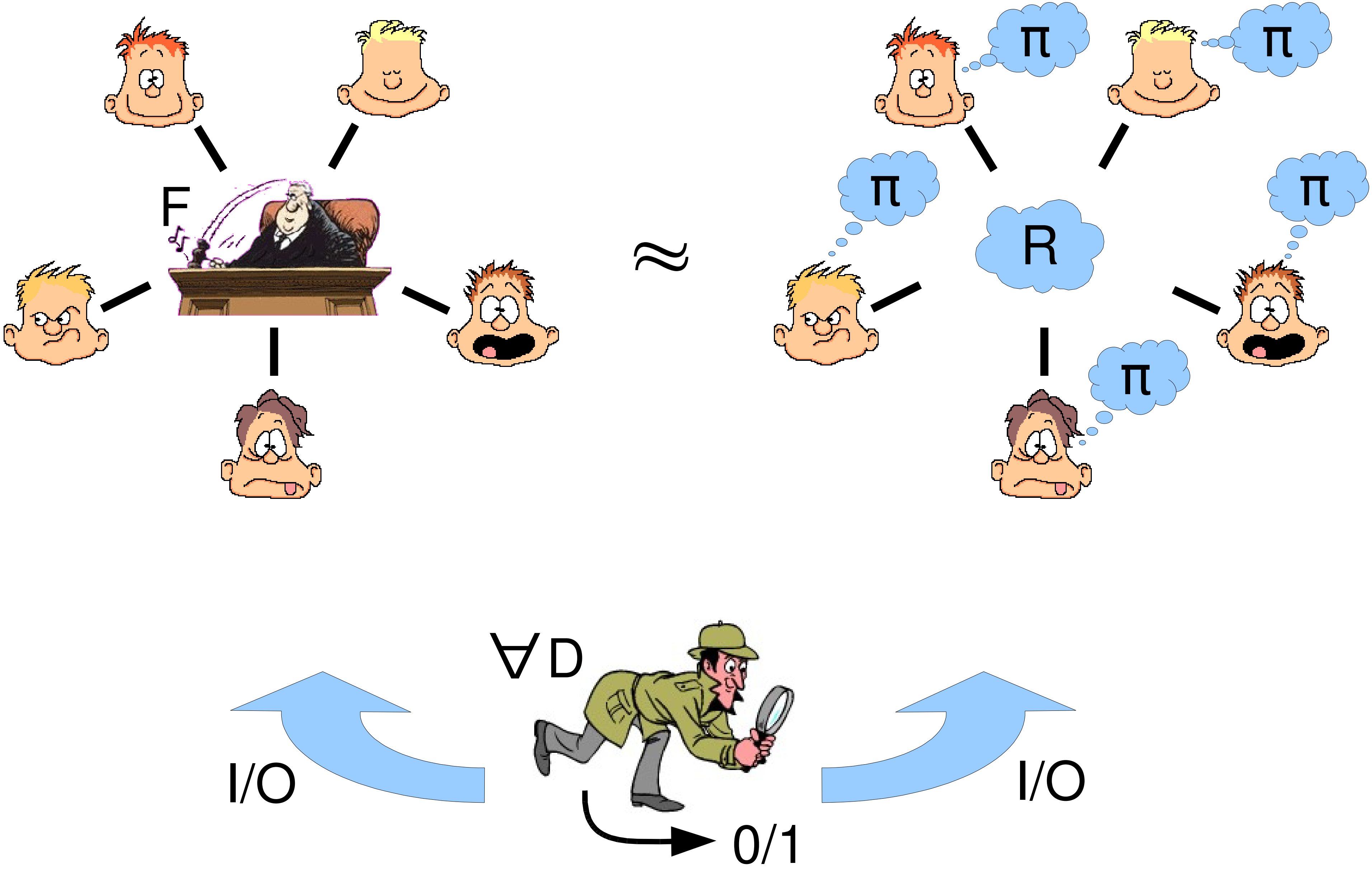
Multi-Party Computation (MPC)



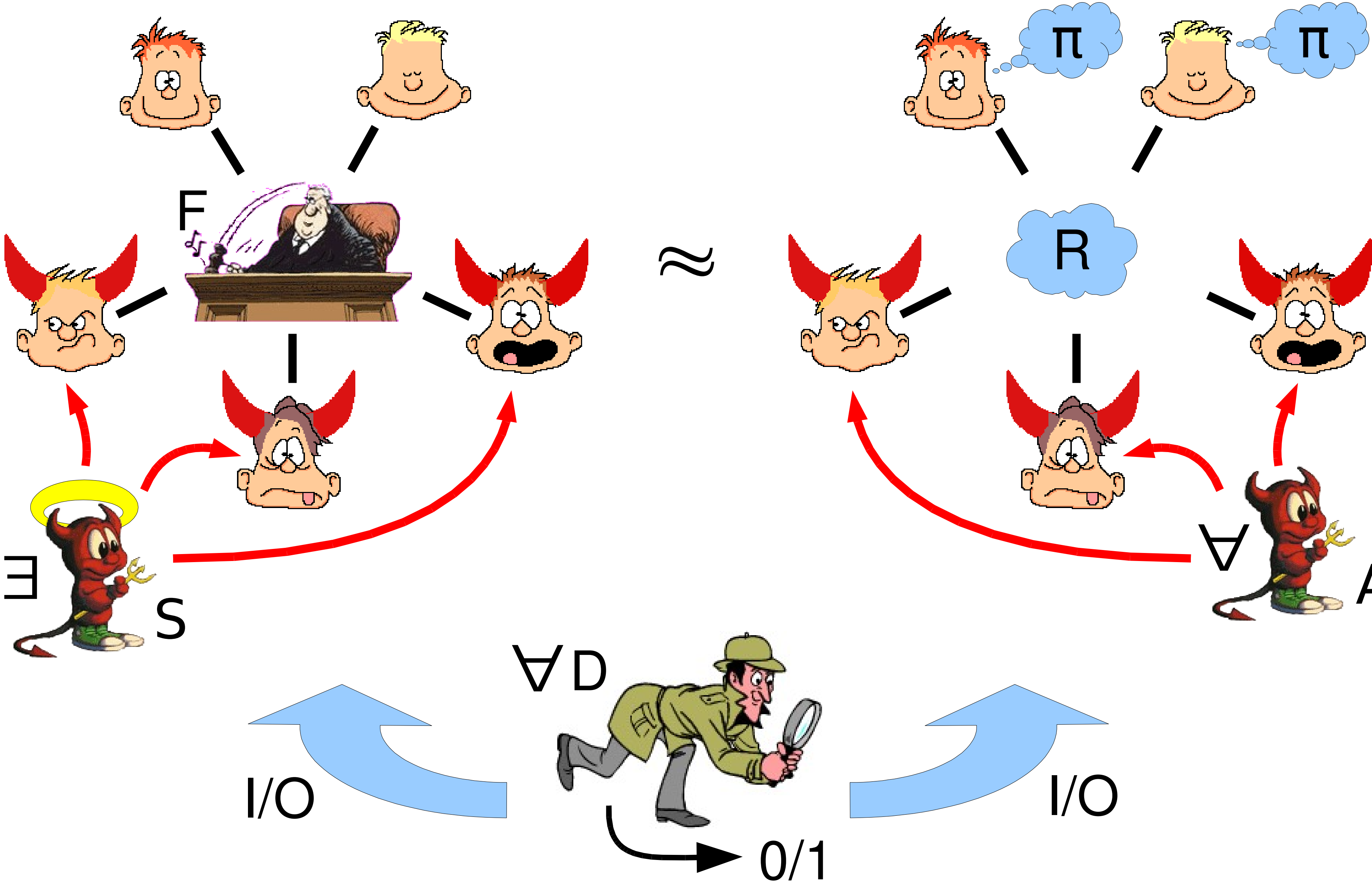
Generally encompasses:

- Secure or authenticated channels
- Optionally BC or PKI
- CRS for UC setting

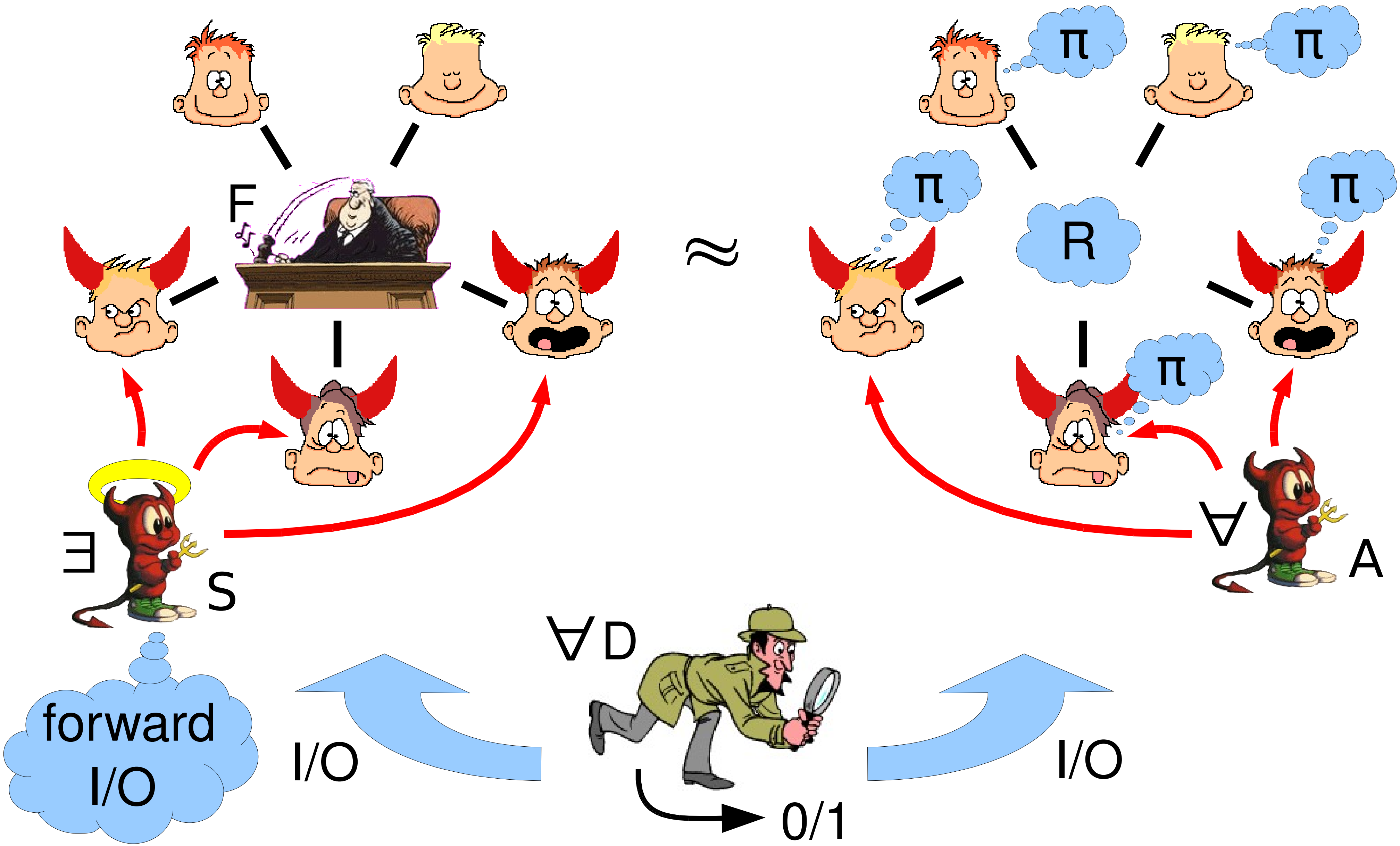
Multi-Party Computation (MPC)



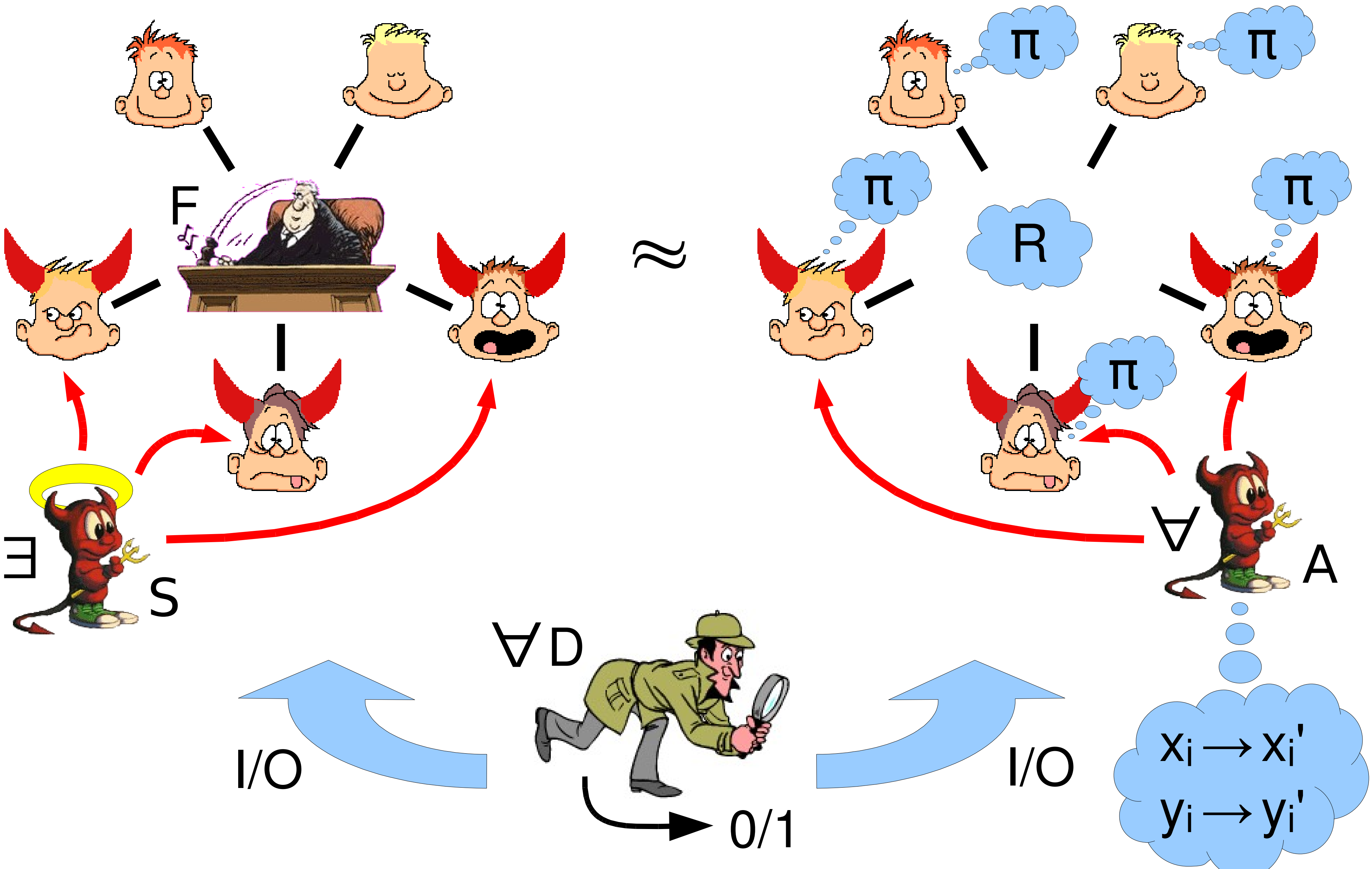
MPC: Active Adversary



MPC: Passive Adversary



MPC: Semi-Honest Adversary



Security Properties for MPC

- Correctness: protocol computes intended result
- Privacy: nobody learns more than intended
- Robustness: everybody receives intended result
- Fairness: everybody receives result, or nobody
- Agreement (on abort): all honest parties receive their result or notification of failure

Security Paradigms for MPC

- Abort Security: agreement, privacy, correctness
- Fair Security: fairness, privacy, correctness
- Full Security: robustness, privacy, correctness

- IT Security: tolerates unbounded adversaries
- CO Security: tolerates computationally bounded adversaries

Limitations for MPC with BC

- Fair security only for $t < n/2$ corrupted [Cle86]
- IT security only for $t < n/2$ [Kil00]
- Full security for t_1 and abort security for t_2 only if $t_1 + t_2 < n$ [IKLP06], [Kat07]

- No IT full security for general MPC for $t \geq n/2$

  ⇒ Which functions can be computed with IT full security for $t \geq n/2$?

  ⇒ Weaker assumptions, graceful degradation?

Limitations for MPC with BC

- Fair security only for $t < n/2$ corrupted [Cle86]
- IT security only for $t < n/2$ [Kil00]
- Full security for t_1 and abort security for t_2 only if $t_1 + t_2 < n$ [IKLP06], [Kat07]

- No IT full security for general MPC for $t \geq n/2$

$\Rightarrow$ Which functions can be computed with IT full security for $t \geq n/2$?

$\Rightarrow$ Weaker assumptions, graceful degradation?

Computability of Functions

Security	Adversary	Resources	Fair?	Computable f
IT	passive	auth. BC	yes	F^{bc}_{pas}
	semi-honest	auth. BC	yes	F^{bc}_{sh}
	active	auth. BC	yes	F^{bc}_{act}

Computability of Functions

Security	Adversary	Resources	Fair?	Computable f
IT	passive	auth. BC	yes	F^{bc}_{pas} $\cap$
	semi-honest	auth. BC	yes	F^{bc}_{sh}
	active	auth. BC	yes	$\cup$ F^{bc}_{act}

Computability of Functions

Security	Adversary	Resources	Fair?	Computable f
IT	passive	auth. BC	yes	F^{bc}_{pas} $\cap$
	semi-honest	auth. BC	yes	F^{bc}_{sh}
	active	auth. BC	yes	$\cup$ F^{bc}_{act}

- Today: only symmetric functions
- Then: $F^{bc}_{sh} = F^{bc}_{pas}$

Computability of Functions

Security	Adversary	Resources	Fair?	Computable f
IT	passive	auth. BC	yes	F^{bc}_{pas} ∩
	semi-honest	auth. BC	yes	F^{bc}_{sh}
	active	auth. BC	yes	∪ F^{bc}_{act}
LT	active	auth. BC	no	F^{bc}_{lts}
		auth. chan.	no	F^{aut}_{lts}
		PKI	no	$F^{ins,pki}_{lts}$

- Long-term (LT) security
  - Computational assumptions only during protocol run

Computability of Functions

Security	Adversary	Resources	Fair?	Computable f
IT	passive	auth. BC	yes	F^{bc}_{pas}
	semi-honest	auth. BC	yes	F^{bc}_{sh}
	active	auth. BC	yes	F^{bc}_{act}
LT	active	auth. BC	no	F^{bc}_{lts}
		auth. chan.	no	F^{aut}_{lts}
		PKI	no	$F^{ins,pki}_{lts}$

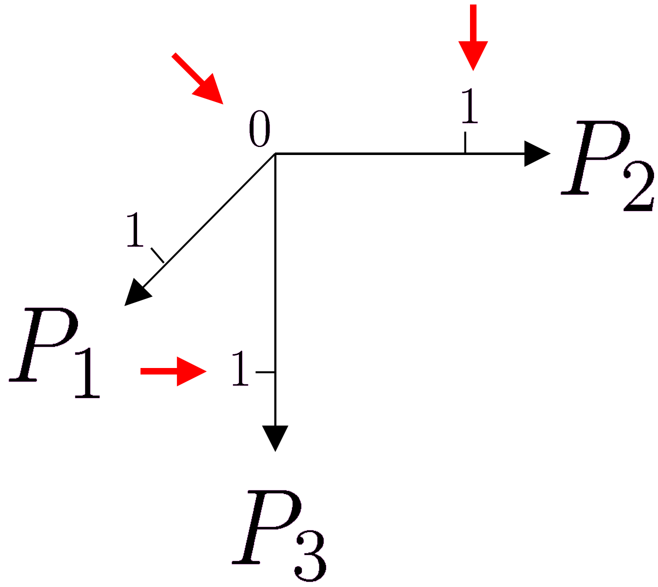
- Long-term (LT) security
  - Computational assumptions only during protocol run

Computability of Functions

Security	Adversary	Resources	Fair?	Computable f
IT	passive	auth. BC	yes	F^{bc}_{pas}
	semi-honest	auth. BC	yes	F^{bc}_{sh}
	active	auth. BC	yes	F^{bc}_{act}
LT	active	auth. BC	no	F^{bc}_{lts}
		auth. chan.	no	F^{aut}_{lts}
		PKI	no	$F^{ins,pki}_{lts}$

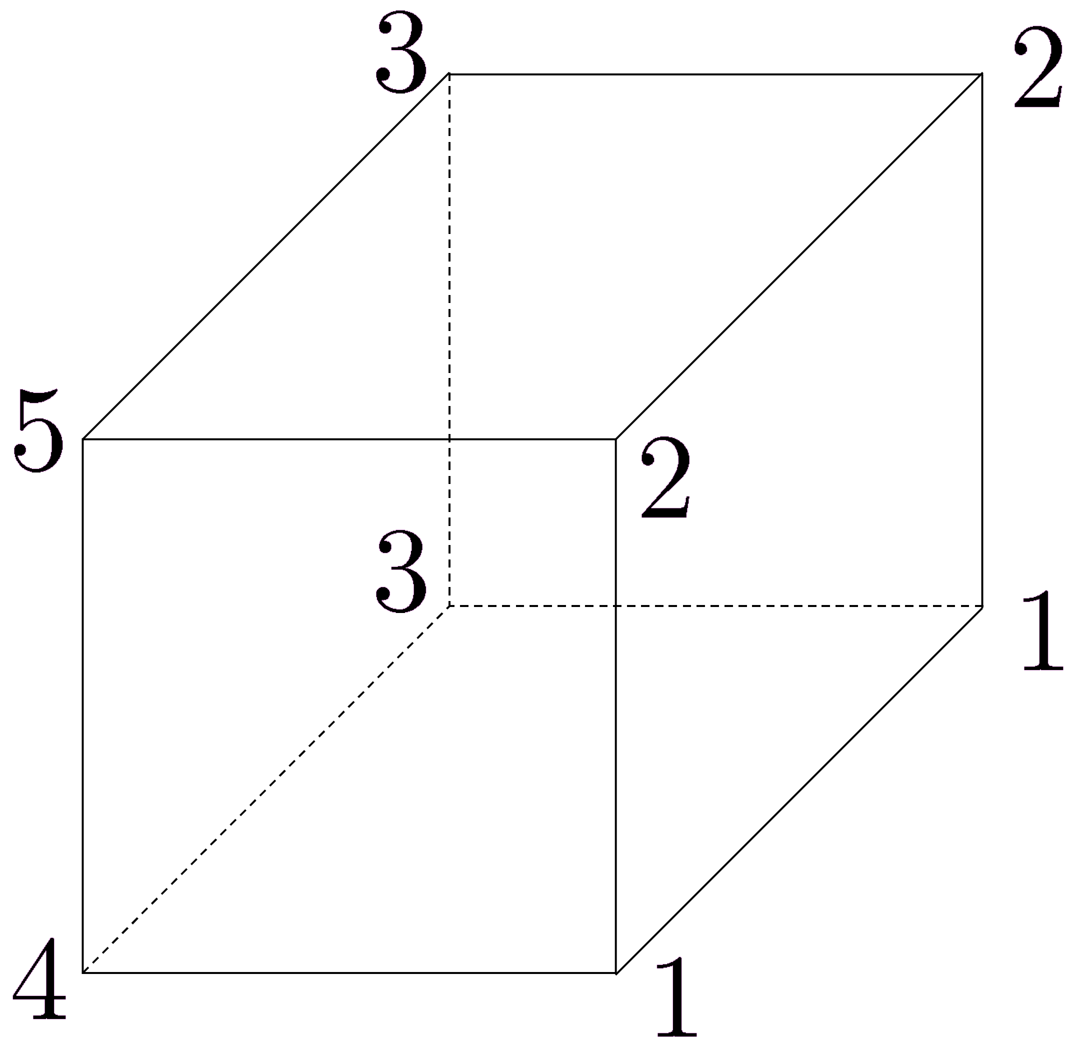
- “=”: modified [GMW87]-Compiler
  - computationally forces semi-honest behavior
  - maintains IT security against semi-honest adversary

Passively Computable Functions F^{bc}_{pas}

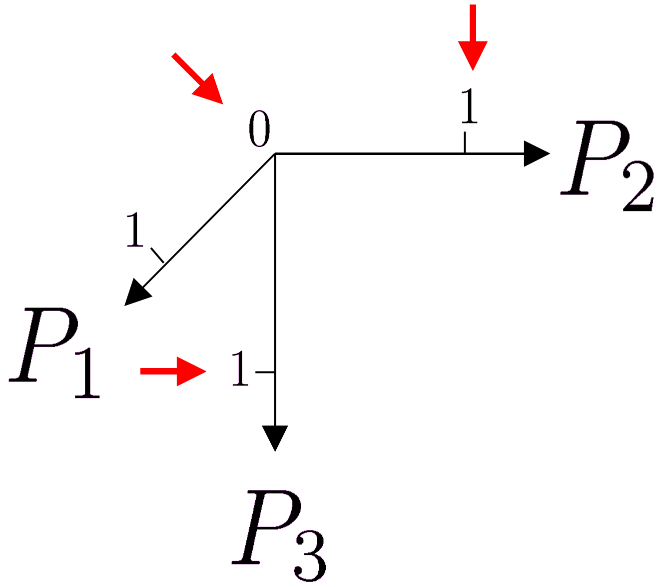


Input:

$\vec{x} = (0, 1, 1)$

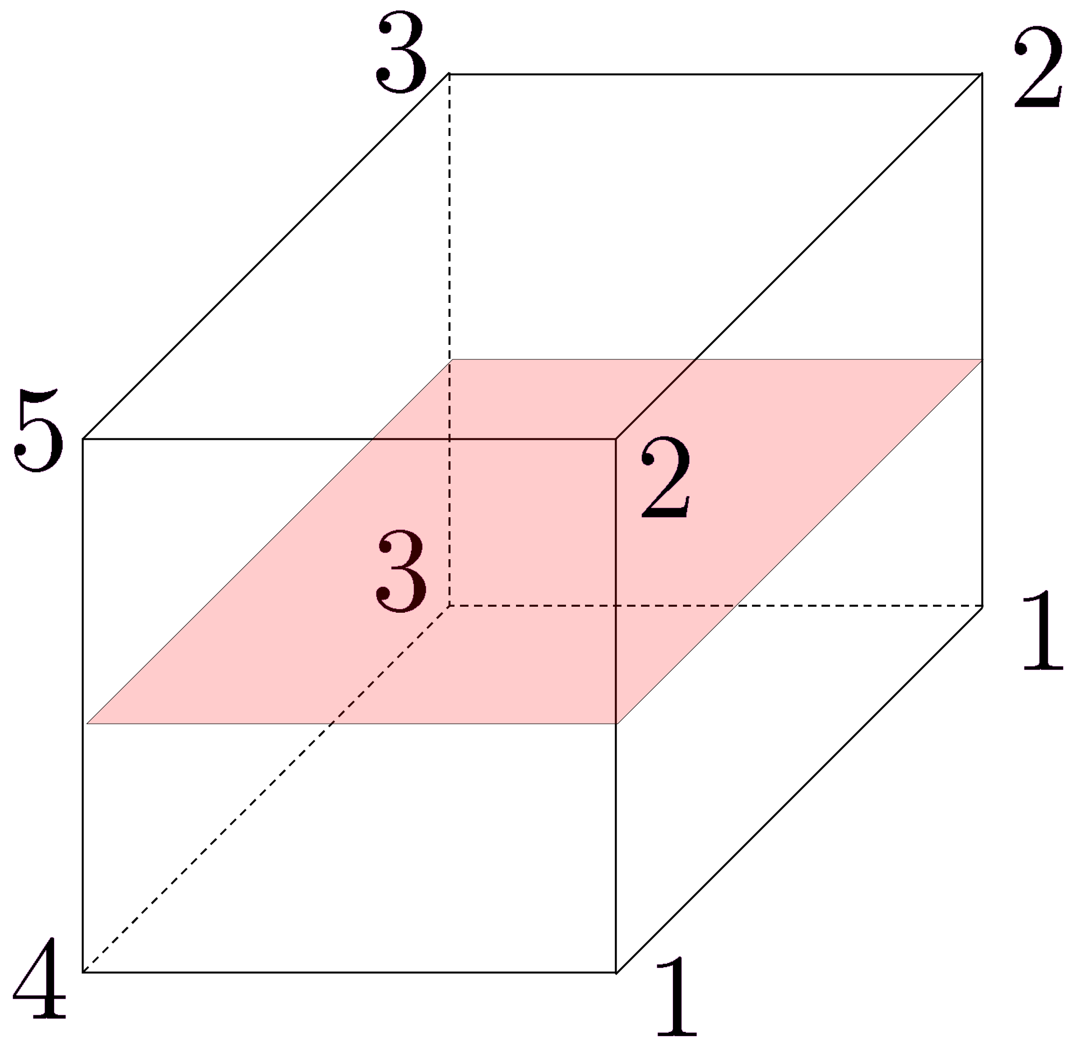


Passively Computable Functions F^{bc}_{pas}

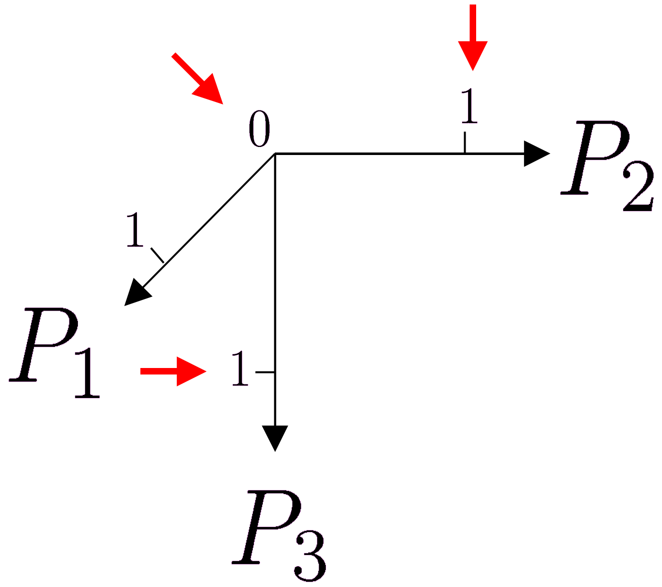


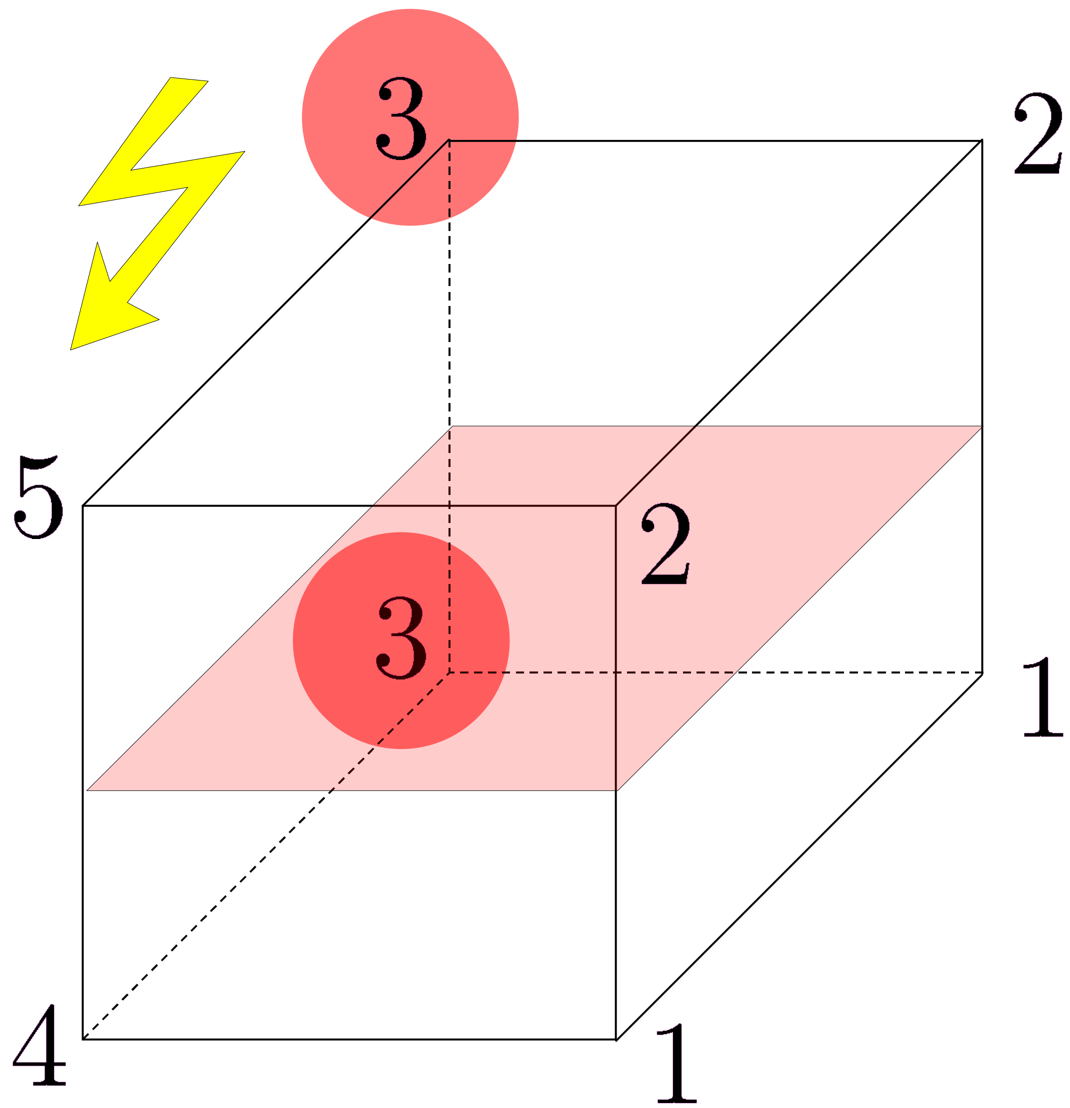
Input:

$$\vec{x} = (0, 1, 1)$$



Passively Computable Functions F^{bc}_{pas}

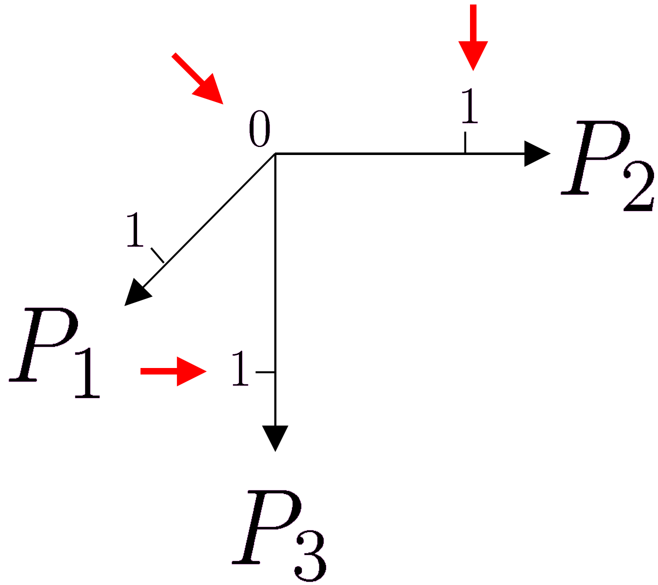




Input:

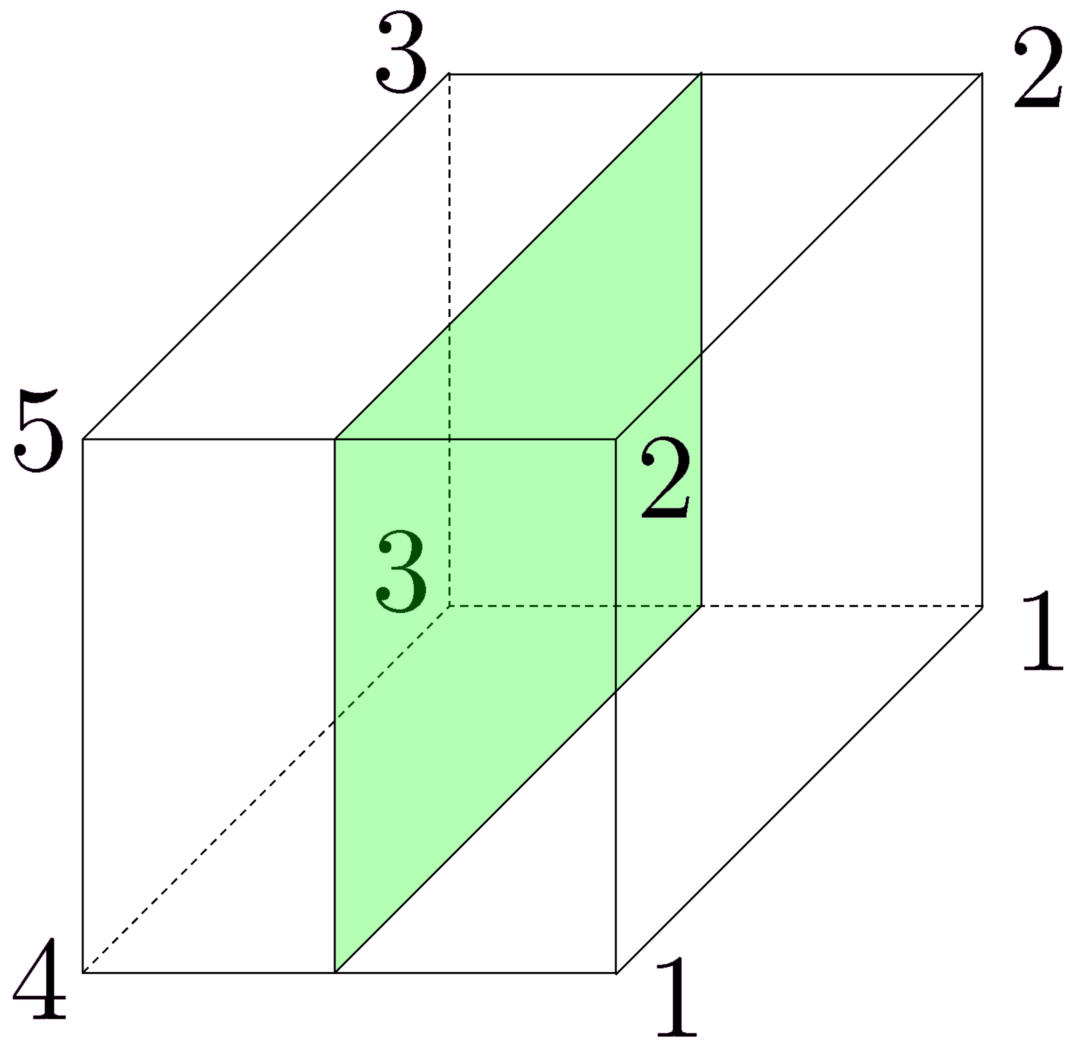
$\vec{x} = (0, 1, 1)$

Passively Computable Functions F^{bc}_{pas}

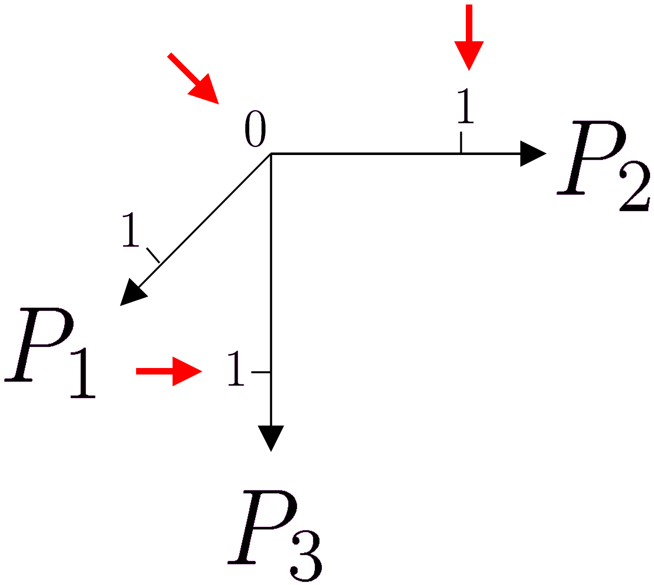


Input:

$$\vec{x} = (0, 1, 1)$$

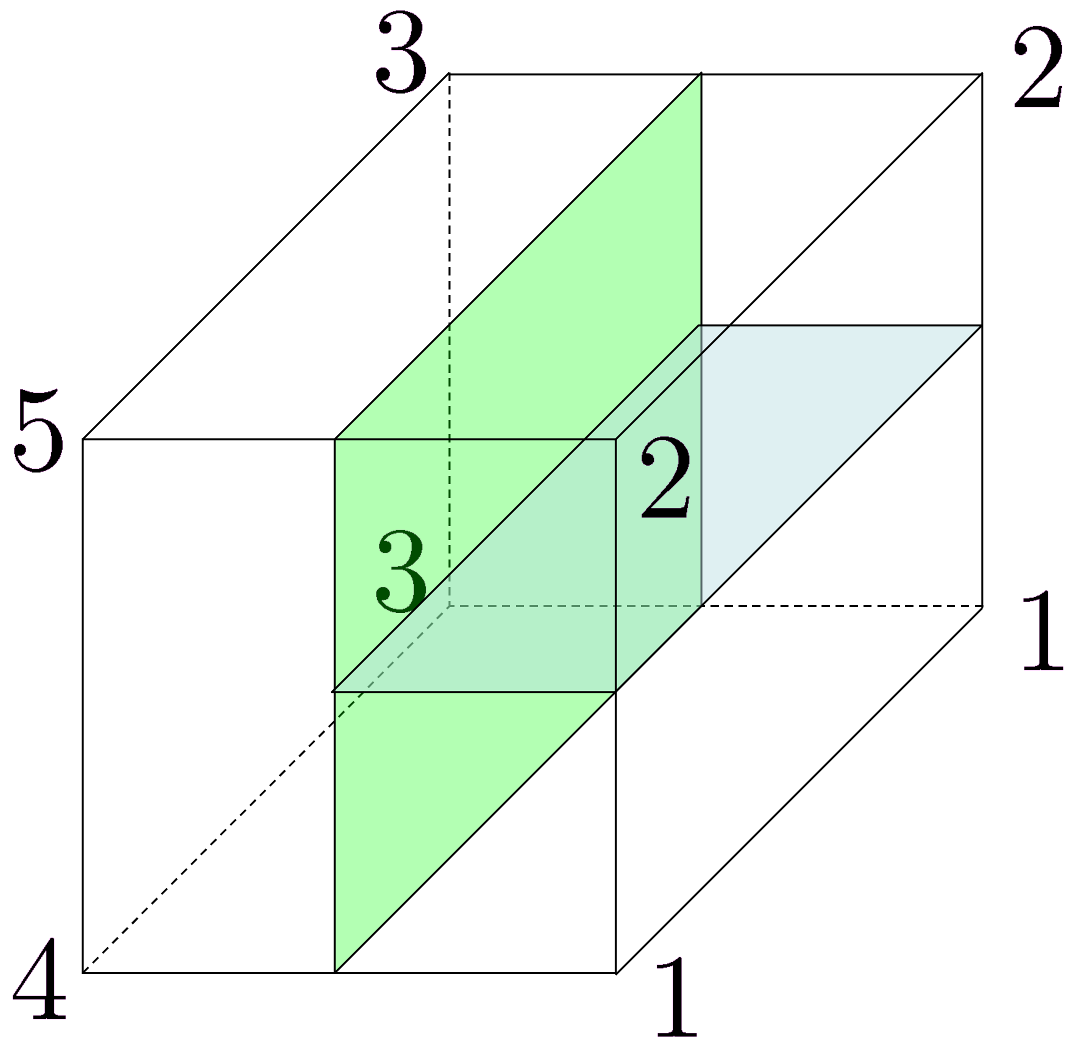


Passively Computable Functions F^{bc}_{pas}

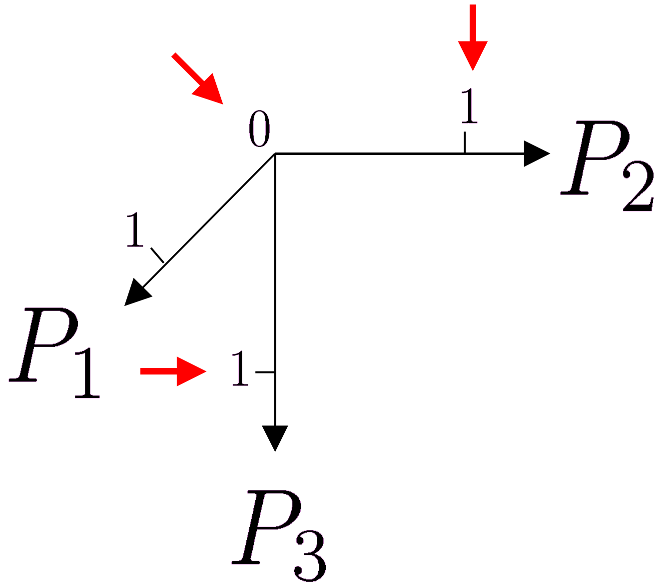


Input:

$$\vec{x} = (0, 1, 1)$$

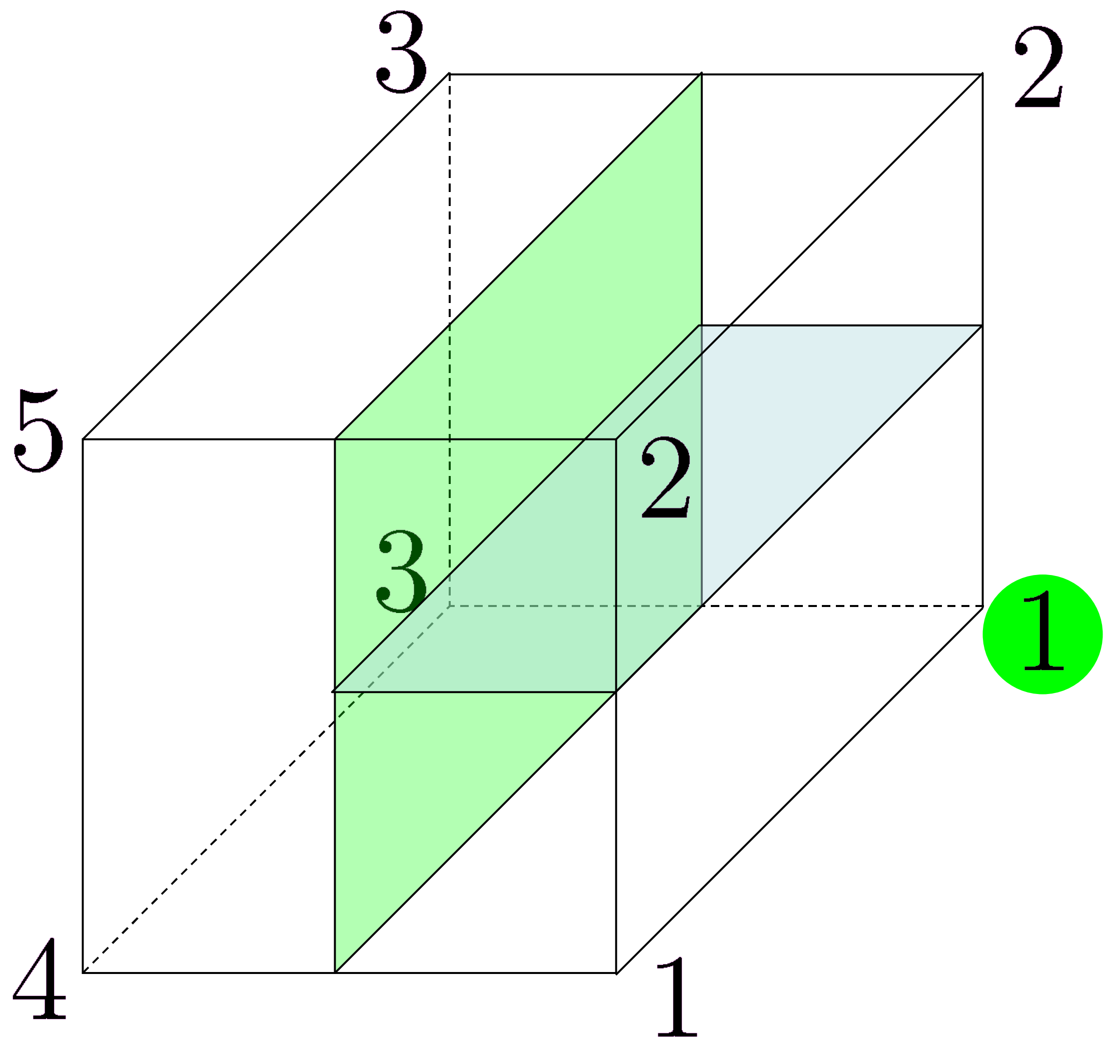


Passively Computable Functions F^{bc}_{pas}

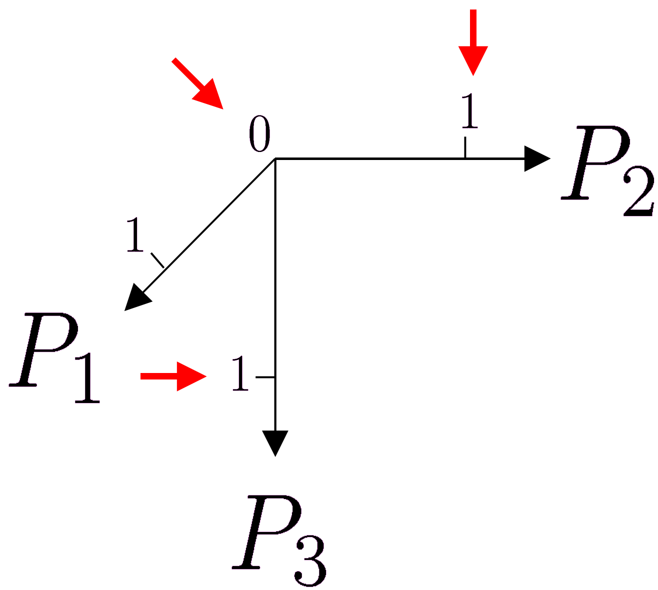


Input:

$$\vec{x} = (0, 1, 1)$$

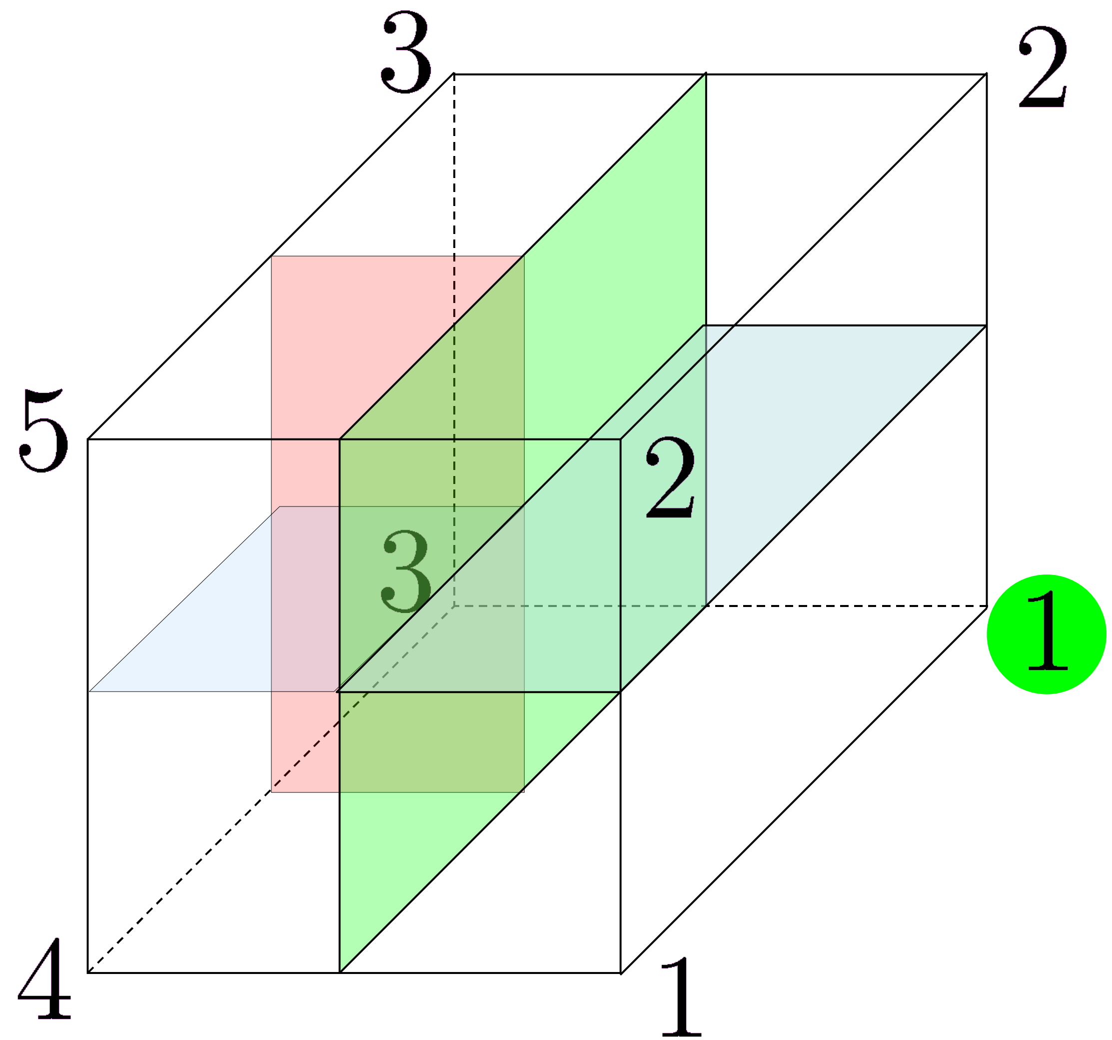


Passively Computable Functions F^{bc}_{pas}

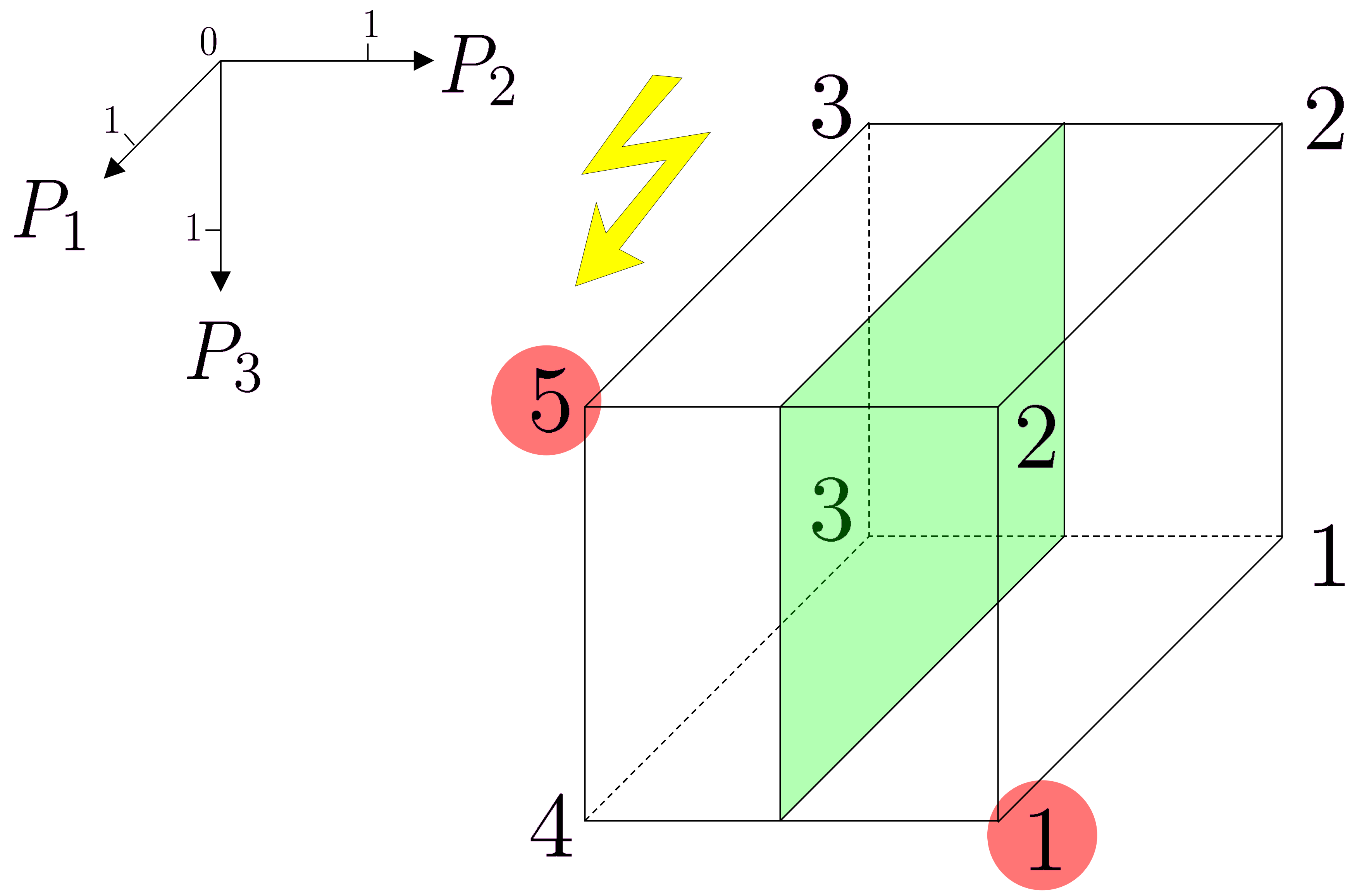


Input:

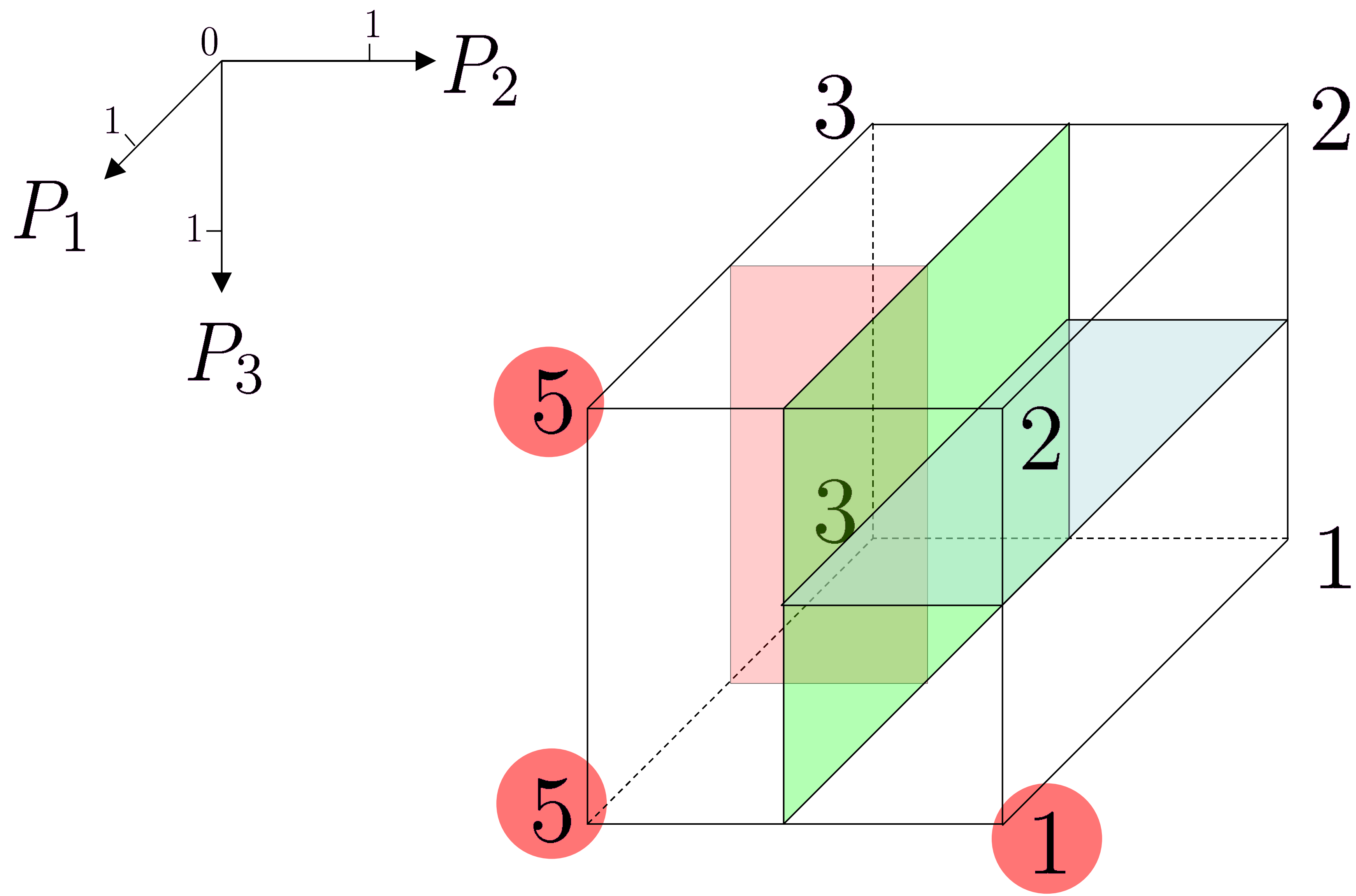
$$\vec{x} = (0, 1, 1)$$



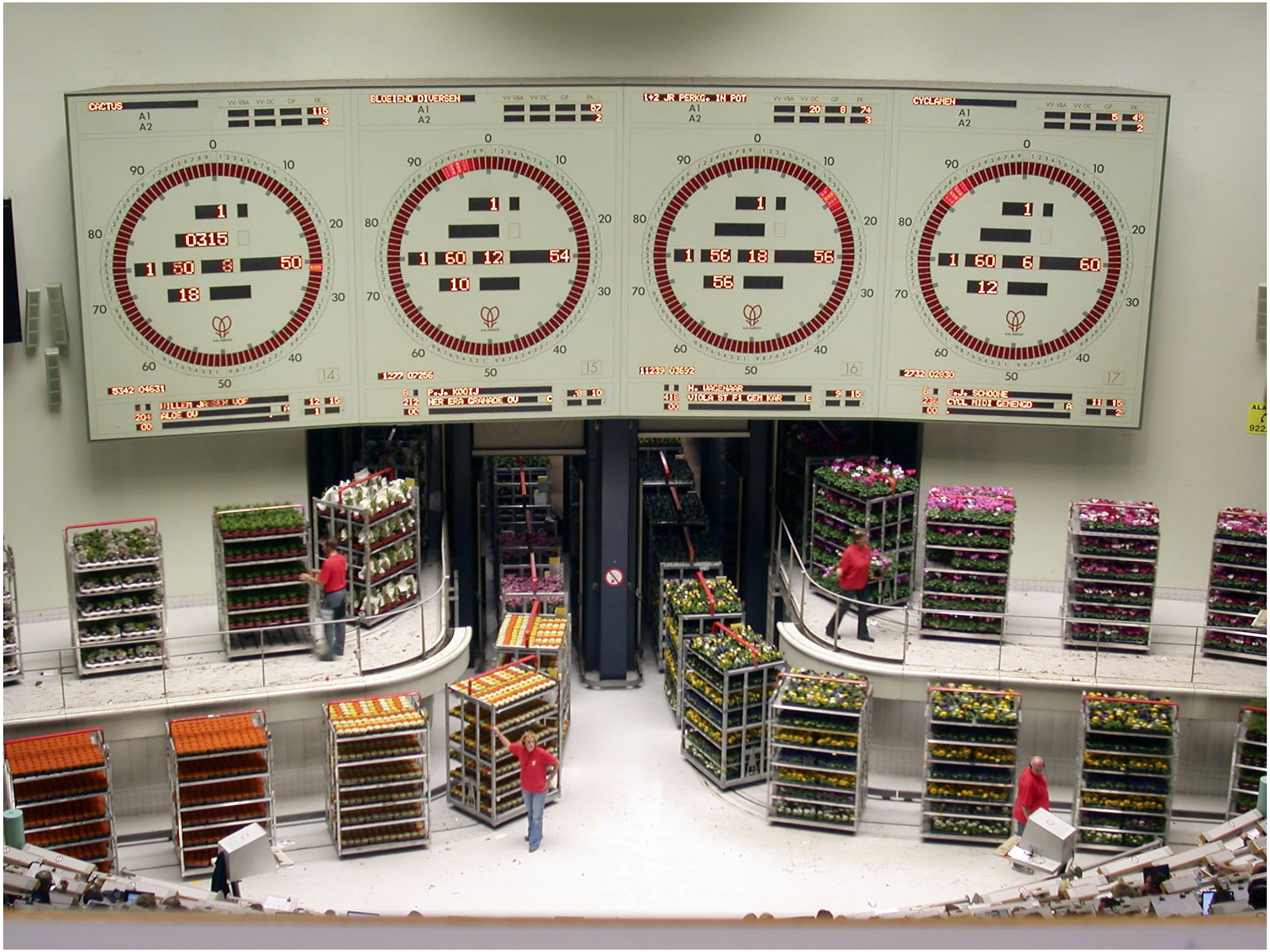
Actively Computable Functions F^{bc}_{act}



Actively Computable Functions F_{act}^{bc}



Actively Computable: Example



Summary: Computability

- Characterization of computable function classes
  - F^{bc}_{pas} : decomposability
  - F^{bc}_{sh} : decomposability after removing redundancy
  - F^{bc}_{act} : decomposability after removing redundancy, exchange property (input for every strategy)
- Characterization of long-term security:

$$F^{ins,pki}_{lts} = F^{aut}_{lts} = F^{bc}_{lts} = F^{bc}_{sh}$$

Limitations for MPC with BC

- Fair security only for $t < n/2$ corrupted [Cle86]
- IT security only for $t < n/2$ [Kil00]
- Full security for t_1 and abort security for t_2 only if $t_1 + t_2 < n$ [IKLP06], [Kat07]

- No IT full security for general MPC for $t \geq n/2$

  ⇒ Which functions can be computed with IT full security for $t \geq n/2$?

  ⇒ Weaker assumptions, graceful degradation?

>

Limitations for MPC with BC

- Fair security only for $t < n/2$ corrupted [Cle86]
- IT security only for $t < n/2$ [Kil00]
- Full security for t_1 and abort security for t_2 only if $t_1 + t_2 < n$ [IKLP06], [Kat07]

- No IT full security for general MPC for $t \geq n/2$

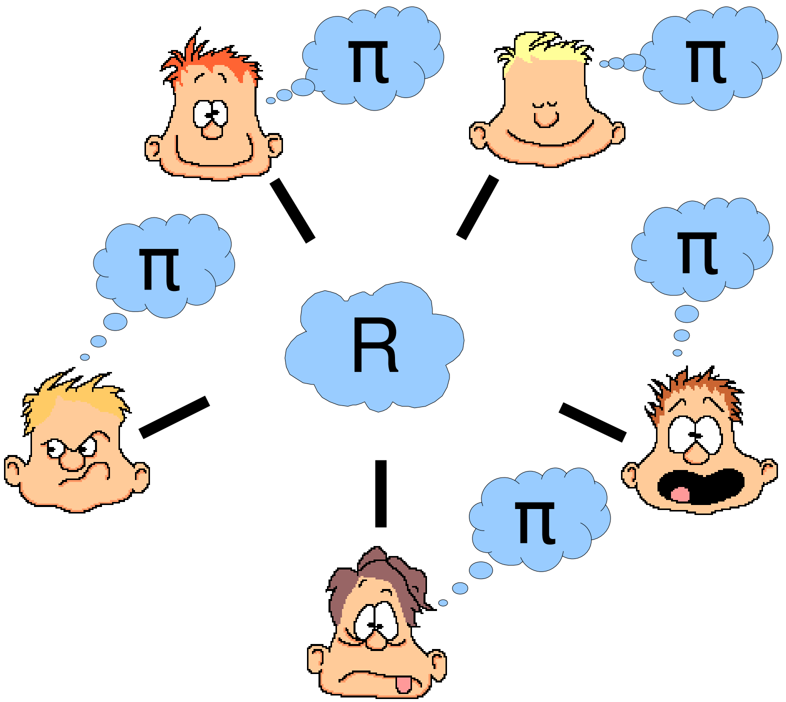
  ⇒ Which functions can be computed with IT full security for $t \geq n/2$?

  ⇒ Weaker assumptions, graceful degradation?

  ⇒ Hybrid-secure MPC (HMPC)

>

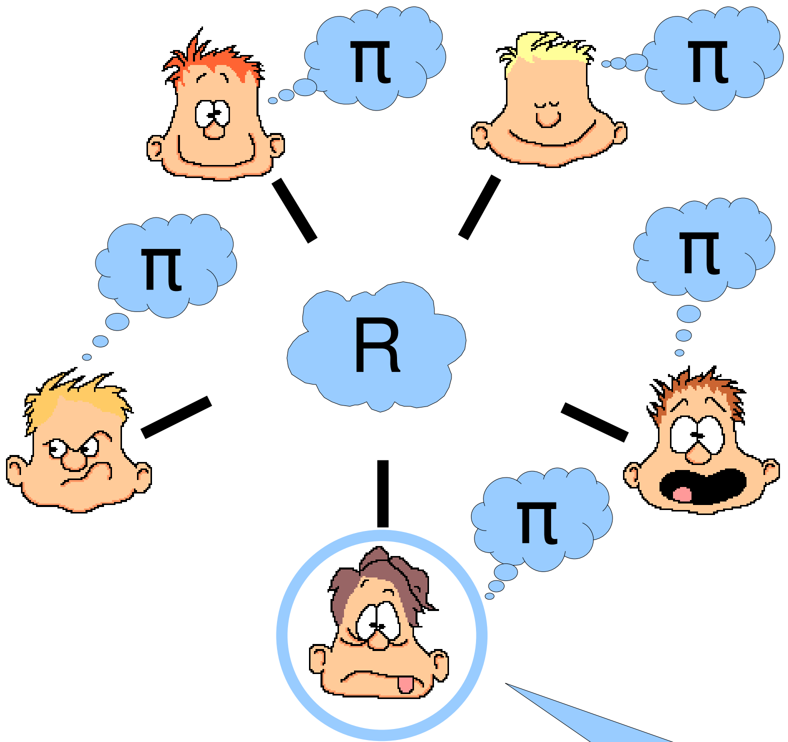
Optimal Hybrid MPC (with BC)



Goal: For any $\rho < n/2$

- IT full security for $t \leq \rho$
- IT fair security for $t < n/2$
- CO abort security for $t < n-\rho$

Optimal Hybrid MPC (with BC)

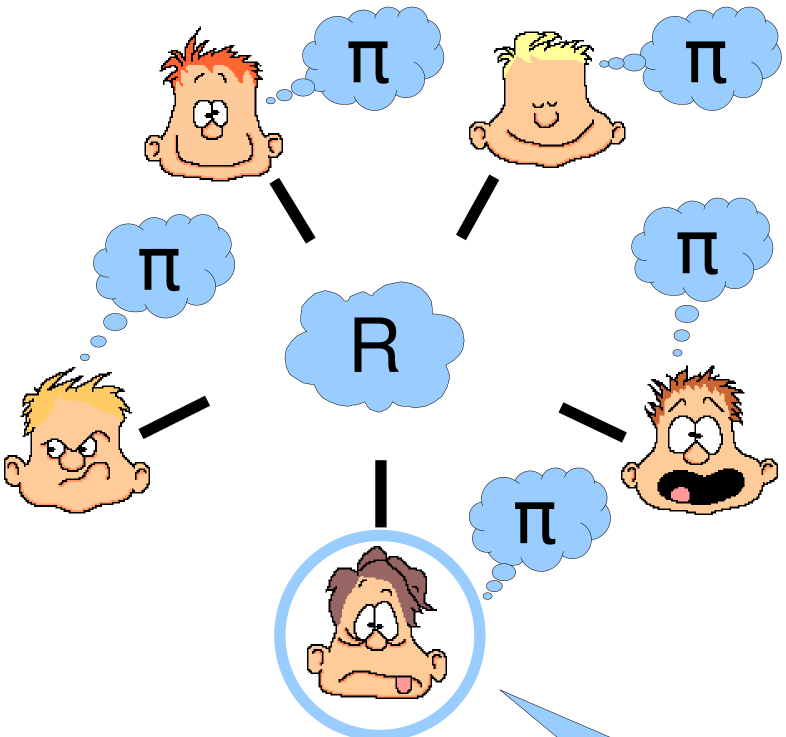


Goal: For any ρ < n/2

- IT full security for t ≤ ρ
- IT fair security for t < n/2
- CO abort security for t < n-ρ

[GMW87], [CLOS01]:
can be IT protected

Optimal Hybrid MPC (with BC)



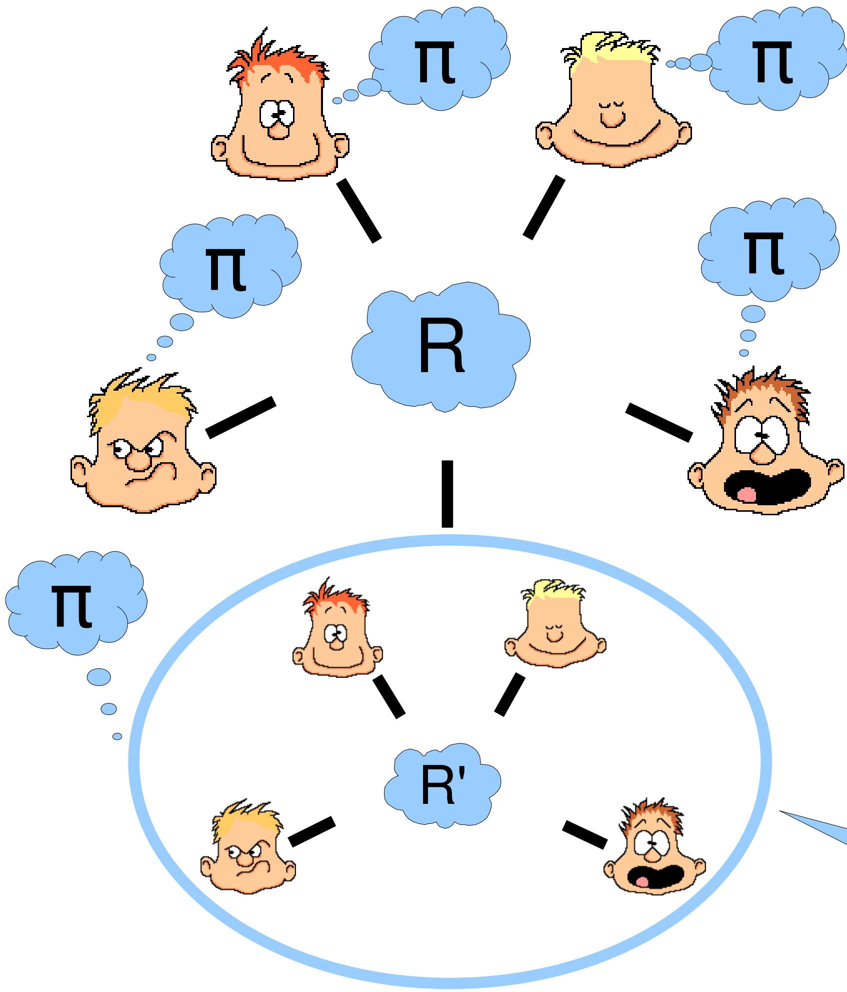
Trusted ⇒
IT fairness, correctness

Goal: For any $\rho < n/2$

- IT full security for $t \leq \rho$
- IT fair security for $t < n/2$
- CO abort security for $t < n-\rho$

>

Optimal Hybrid MPC (with BC)



[Cha89]: emulate!

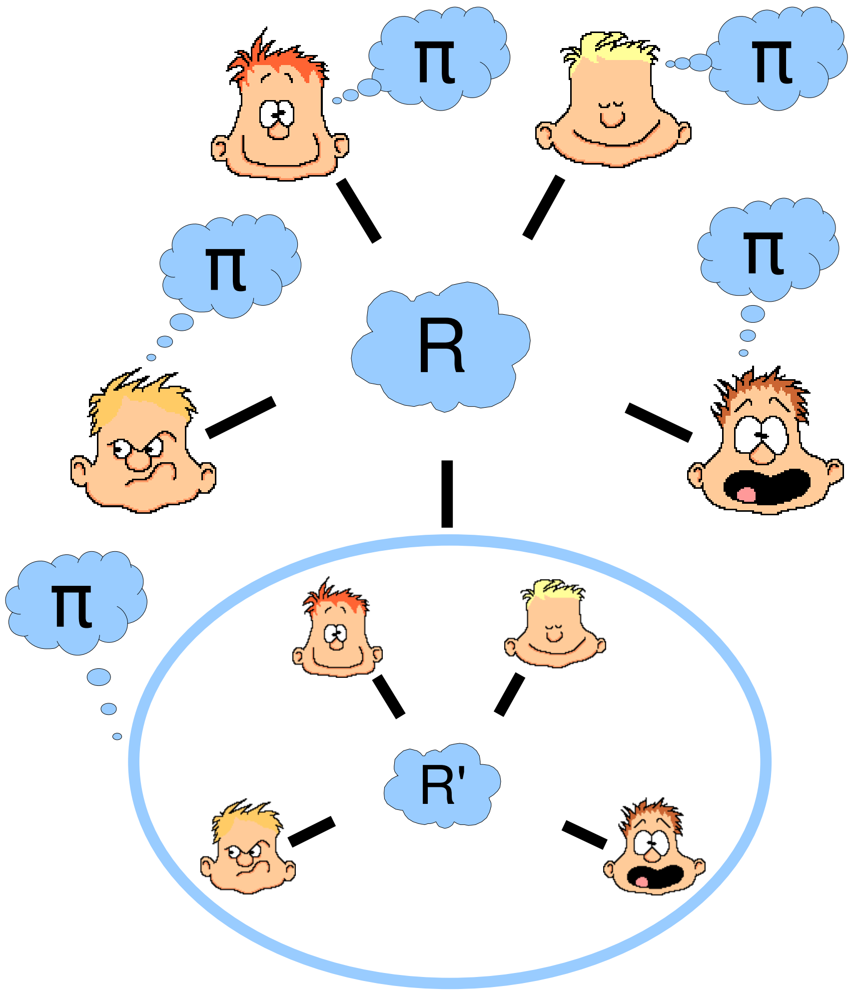
⇒ honest for $t < n/2$ [RB89]

⇒ $t < n/2$: IT fair, correct

⇒ $t \geq n/2$: CO private, correct

Trusted ⇒
IT fairness, correctness

Optimal Hybrid MPC (with BC)



[Cha89]: emulate!

⇒ honest for $t < n/2$ [RB89]

⇒ $t < n/2$: IT fair, correct

⇒ $t \geq n/2$: CO private, correct

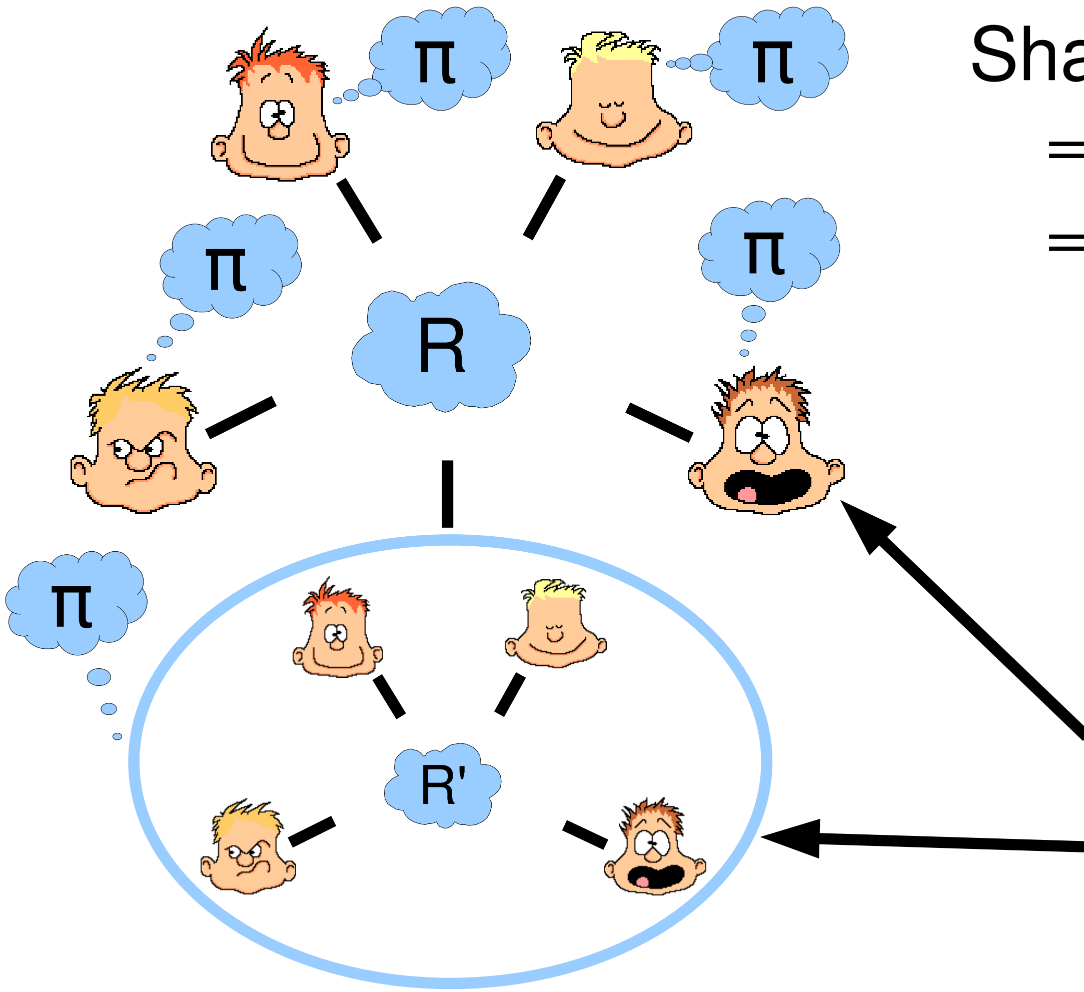
Use sharing qualifying all sets of emulated and n-ρ actual parties

⇒ $t \leq \rho$: IT robust, correct

⇒ $t < n/2$: IT fair, correct

⇒ $t < n-\rho$: CO private, correct

Optimal Hybrid MPC (with BC)



Share inputs

⇒ $t < n/2$: IT privacy

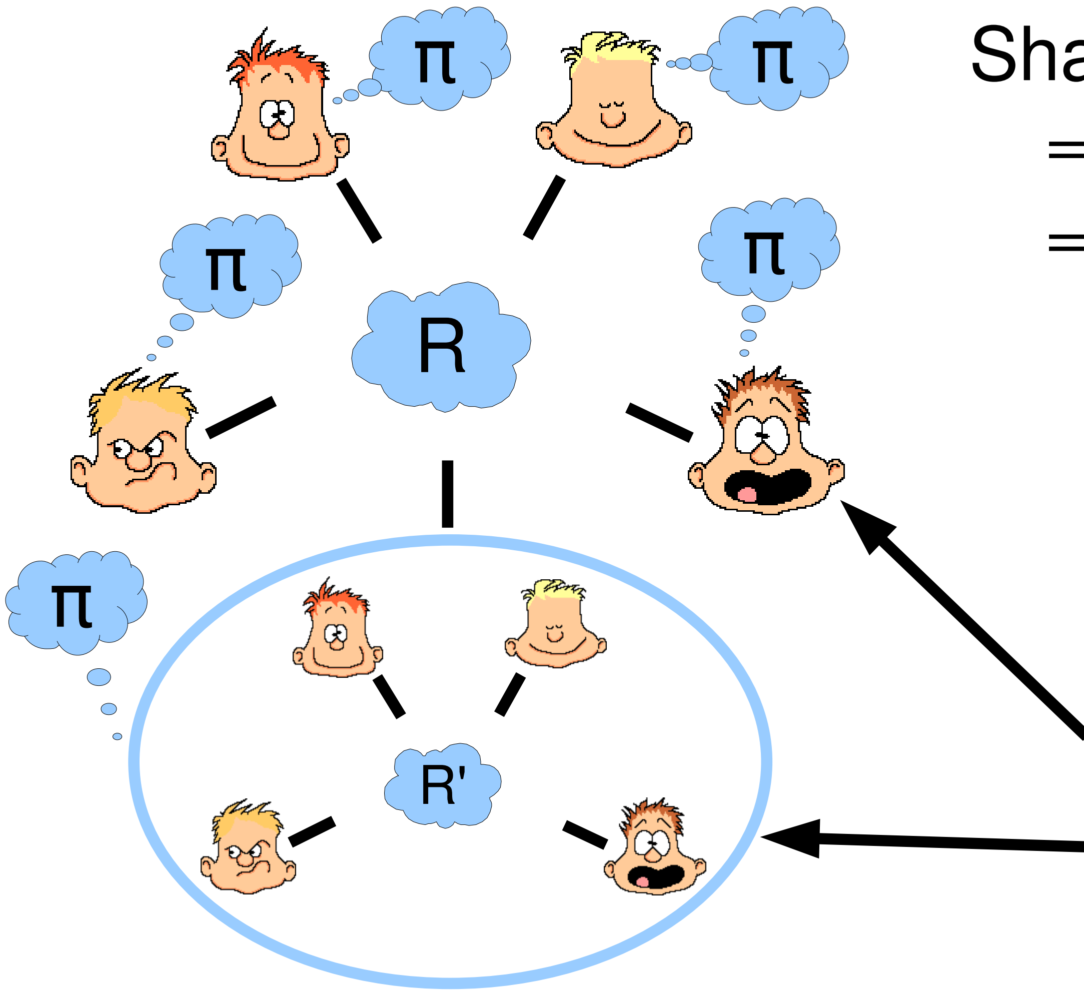
⇒ $t \geq n/2$: no correctness

$x_i = x_i^{des} \oplus x_i^{em}$

(x_i^{des})

(x_i^{em})

Optimal Hybrid MPC (with BC)



Share and commit

⇒ no robustness or

⇒ no correctness for $t \geq n/2$

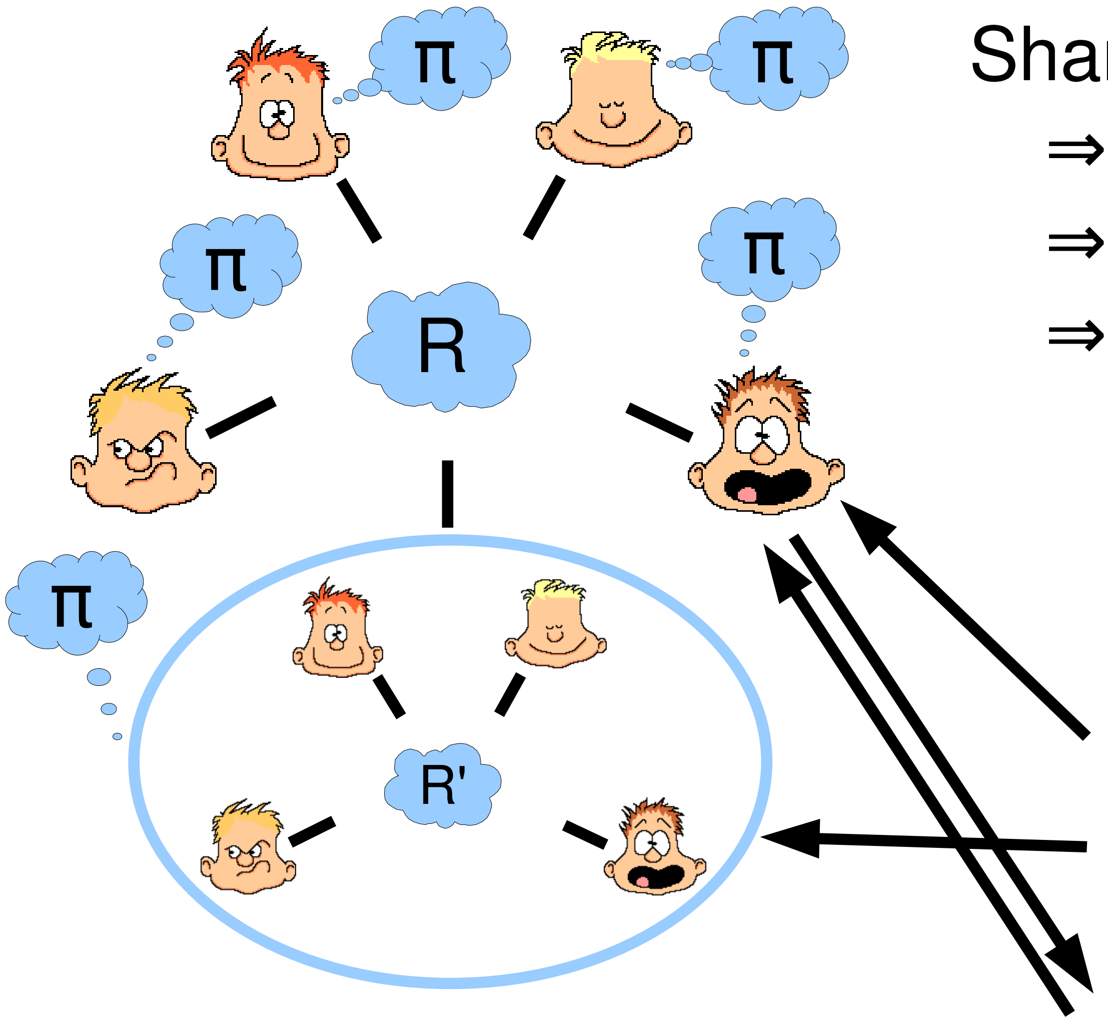
$x_i = x_i^{des} \oplus x_i^{em}$

$(c_i, o_i) = com_H(x_i^{em})$

(x_i^{des}, c_i)

(x_i^{em}, o_i)

Optimal Hybrid MPC (with BC)



Share, commit, complain

- $\Rightarrow t \leq \rho$: IT full security
- $\Rightarrow t < n/2$: IT fair security
- $\Rightarrow t < n\text{-}\rho$: CO abort security

$x_i = x_i^{des} \oplus x_i^{em}$

$(c_i, o_i) = com_H(x_i^{em})$

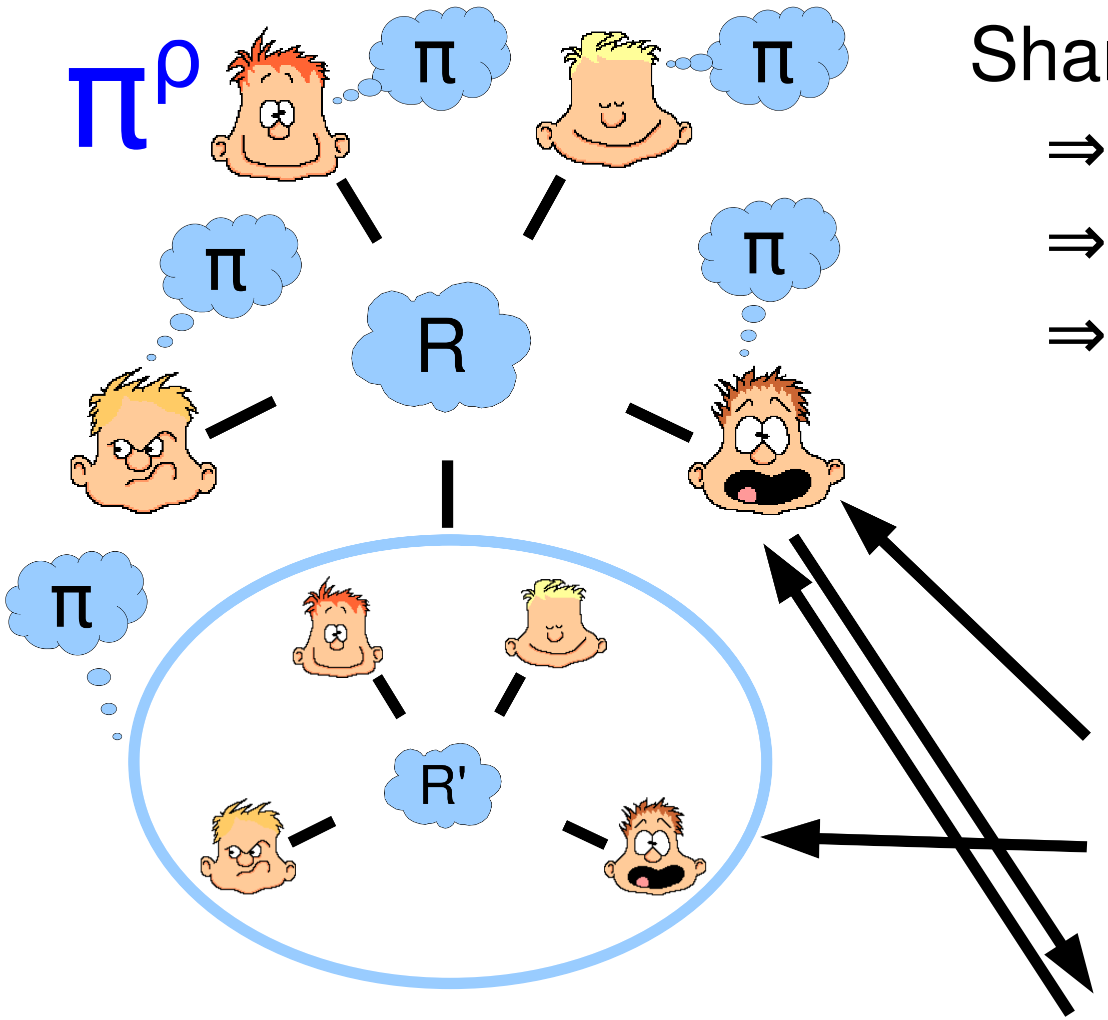
(x_i^{des}, c_i)

(x_i^{em}, o_i)

complaint? input x_i

>

Optimal Hybrid MPC (with BC)



Share, commit, complain

- $\Rightarrow t \leq \rho$: IT full security
- $\Rightarrow t < n/2$: IT fair security
- $\Rightarrow t < n-\rho$: CO abort security

$x_i = x_i^{des} \oplus x_i^{em}$

$(c_i, o_i) = com_H(x_i^{em})$

(x_i^{des}, c_i)

(x_i^{em}, o_i)

complaint? input x_i

Summary: Hybrid Security

- We provide optimal HMPC protocols and matching tight bounds for the setting
  - with BC

Summary: Hybrid Security

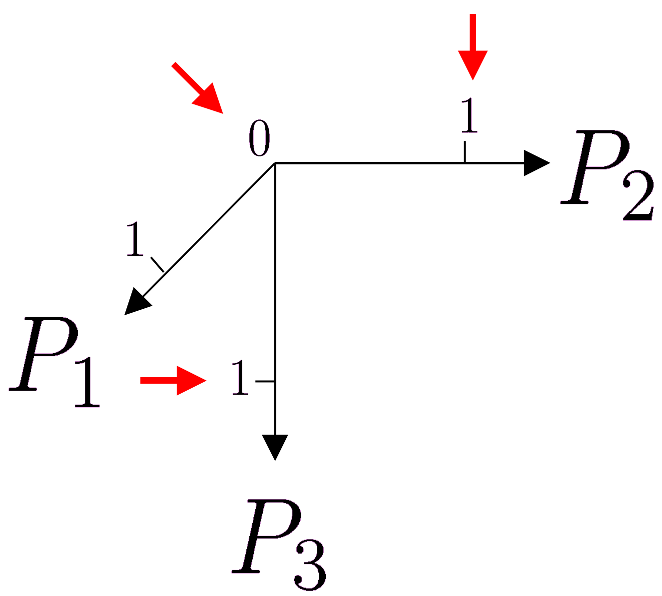
- We provide optimal HMPC protocols and matching tight bounds for the setting
  - with BC
  - without BC but with PKI
  - without BC or PKI
- We treat possibly inconsistent PKIs
- We consider signature forgery separately from other (computational) assumptions

Conclusions

- Characterization of computable function classes
- Characterization of long-term security

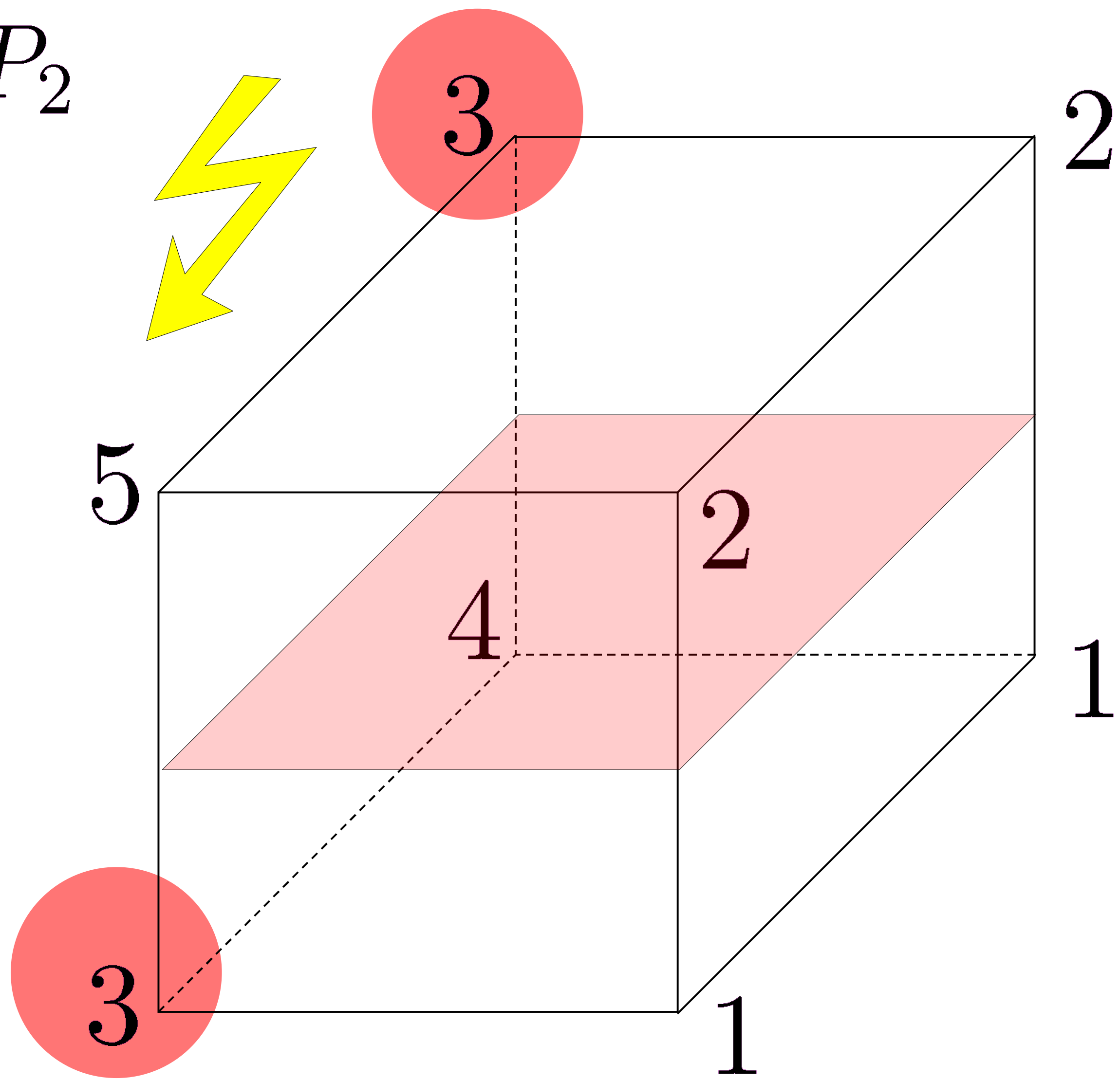
- Optimal HMPC protocols and matching tight bounds

Passively Computable Functions F^{bc}_{pas}



Input:

$\vec{x} = (0, 1, 1)$



Hybrid MPC (HMPC)

- Different guarantees depending on t:
  - For $t \leq l_r$ full (robust) security
  - For $t \leq l_f$ fair security
  - For $t \leq L$ abort security
- While tolerating:
  - For $t \leq t_c$ computationally unbounded adversaries
  - For $t \leq t_\sigma$ signature forgery
  - For $t \leq t_p$ inconsistent PKIs

⇒ Graceful degradation

Summary: Hybrid Security

- We provide HMPC protocols for the setting
  - with BC under the bounds
    $t_c < n/2 \ \wedge \ l_r \leq l_f \leq L \ \wedge \ l_f < n/2 \ \wedge \ l_r + L < n$
  - without BC but with PKI under the bounds
    $t_c < n/2 \ \wedge \ l_r \leq l_f \leq L \ \wedge \ l_f < n/2 \ \wedge \ l_r + L < n$
    $\wedge \ 2 t_\sigma + L < n \ \wedge \ (t_p > 0 \Rightarrow t_p + 2L < n)$
  - without BC or PKI under the bounds
    $t_c < n/2 \ \wedge \ l_r \leq l_f \leq L \ \wedge \ l_f < n/2 \ \wedge \ (l_r > 0 \Rightarrow l_r + 2L < n)$
- Our bounds are tight, given $l_r \geq t_p, t_\sigma$

Limitations for HMPC with BC

- IT security for $t \leq t_c$ only if $t_c < n/2$ [Kil00]
- Fair security for $t \leq l_f$ only if $l_f < n/2$ [Cle86]
- Full security for $t \leq l_r$ and abort security for $t \leq L$ only if $l_r + L < n$ [IKLP06], [Kat07]

- Therefore:
  $$t_c < n/2 \;\wedge\; l_r \leq l_f \leq L \;\wedge\; l_f < n/2 \;\wedge\; l_r + L < n \qquad (1)$$

Hybrid MPC without BC or PKI

- Fair security for $t \le l_f$ only if $l_f < n/2$ [Cle86]
- IT security for $t \le t_c$ only if $t_c < n/2$ [Kil00]
- Full security for $t \le l_r$ and abort security for $t \le L$ only if $l_r > 0 \Rightarrow l_r+2L < n$ [FHHW03]
- Protocol π^ρ with the BC from [FHHW03] achieves bound $t_c < n/2 \;\wedge\; l_r \le l_f \le L \;\wedge\; l_f < n/2 \;\wedge\; (l_r > 0 \Rightarrow l_r+2L < n)$ (2)
- Improves over [FHHW03] for $\rho=0$, which makes no guarantees for $t > n/2$

Limits for MPC without BC, with PKI

- Tolerate inconsistent PKI for $t \leq t_p$
- Tolerate signature forgery for $t \leq t_\sigma$

- We achieve the following bounds

$$t_c < n/2 \;\wedge\; l_r \leq l_f \leq L \;\wedge\; l_f < n/2 \;\wedge\; l_r + L < n$$
$$\wedge\; 2t_\sigma + L < n \;\wedge\; (t_p > 0 \Rightarrow t_p + 2L < n) \quad (3)$$

and prove them necessary for $l_r \geq t_p, t_\sigma$

Hybrid MPC without BC, with PKI

- Protocol π^{ρ} with a hybrid BC (HBC) for bounds $2t_{\sigma}+T < n \;\wedge\; (t_p > 0 \Rightarrow t_p+2T < n)$ achieves bound (3) (where BC secure for $t \leq T$)
- For $t_p > 0$ treated in [FHW04]
- For $t_p = 0$ and $2t_{\sigma}+T < n$ we provide an HBC protocol achieving full BC
  - For $t = 0$ unconditionally
  - For $t \leq t_{\sigma}$ conditional on PKI consistency
  - For $t \leq T$ conditional on unforgeability and PKI consistency

BC with extended validity (BCEV)

- For $2t_\sigma + T < n$ and $t_p = -1$ BCEV achieves:
  - For $t \leq t_\sigma$ full broadcast
  - For $t \leq T$ validity, conditional on unforgeability

BC with extended validity (BCEV)

- For $2t_\sigma + T < n$ and $t_p = -1$ BCEV achieves:
  - For $t \leq t_\sigma$ full broadcast
  - For $t \leq T$ validity, conditional on unforgeability

1. P_s: multisend $(m, \sigma_s(m))$; [receive (x_i, σ_i)]
2. $\forall \text{P}_i$: $\text{BGP}((x_i, \sigma_i))$; [$\forall \text{P}_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]

   $S_i^{v,0} := \{j | v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{valid}\}$;

   $S_i^v := \{j | v_i^j = v \wedge \sigma_i^j \text{valid}\}$;
3. $\texttt{if}\ |S_i^{x_i,0}| \geq n - T\ \wedge\ |S_i^{1-x_i}| = 0\ \texttt{then}\ y_i := x_i$ (I)

   $\texttt{elsif}\ |S_i^0| > |S_i^1|\ \texttt{then}\ y_i := 0\ \texttt{else}\ y_i := 1\ \texttt{fi}.$ (II)

BCEV: Validity for t ≤ T

1. P_s: multisend $(m, \sigma_s(m))$; [receive (x_i, σ_i)]
2. $\forall \mathsf{P}_i$: $\mathrm{BGP}((x_i, \sigma_i))$; [$\forall \mathsf{P}_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]

   $S_i^{v,0} := \{j | v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{valid}\};$

   $S_i^{v} := \{j | v_i^{j} = v \wedge \sigma_i^{j} \text{valid}\};$
3. $\texttt{if } |S_i^{x_i,0}| \geq n - T \ \wedge \ |S_i^{1-x_i}| = 0 \texttt{ then } y_i := x_i$ (I)

   $\texttt{elsif } |S_i^0| > |S_i^1| \texttt{ then } y_i := 0 \texttt{ else } y_i := 1 \texttt{ fi.}$ (II)

BCEV: Validity for t ≤ T

validity:
P_s honest

1. P_s: multisend $(m, \sigma_s(m))$; [receive (x_i, σ_i)]

2. $\forall \mathsf{P}_i$: BGP$((x_i, \sigma_i))$; [$\forall \mathsf{P}_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]

$$S_i^{v,0} := \{j | v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{valid}\};$$

$$S_i^{v} := \{j | v_i^{j} = v \wedge \sigma_i^{j} \text{valid}\};$$

3. $\texttt{if } |S_i^{x_i,0}| \geq n - T \;\wedge\; |S_i^{1-x_i}| = 0 \texttt{ then } y_i := x_i$ (I)

$\texttt{elsif } |S_i^0| > |S_i^1| \texttt{ then } y_i := 0 \texttt{ else } y_i := 1 \texttt{ fi.}$ (II)

BCEV: Validity for t ≤ T

validity: P_s honest

= $(m, \sigma_s(m))$

1. P_s: multisend $(m, \sigma_s(m))$; [receive (x_i, σ_i)]

2. $\forall \mathsf{P}_i$: BGP$((x_i, \sigma_i))$; [$\forall \mathsf{P}_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]

$S_i^{v,0} := \{j | v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{valid}\}$;

$S_i^v := \{j | v_i^j = v \wedge \sigma_i^j \text{valid}\}$;

3. **if** $|S_i^{x_i,0}| \geq n - T \;\wedge\; |S_i^{1-x_i}| = 0$ **then** $y_i := x_i$ (I)

elsif $|S_i^0| > |S_i^1|$ **then** $y_i := 0$ **else** $y_i := 1$ **fi**. (II)

BCEV: Validity for t ≤ T

validity: P_s honest

for P_j honest = $((m,\sigma_s(m)), ?)$

= $(m,\sigma_s(m))$

1. P_s: multisend $(m, \sigma_s(m))$; [receive (x_i, σ_i)]
2. $\forall \mathsf{P}_i$: BGP$((x_i, \sigma_i))$; [$\forall \mathsf{P}_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]

   $S_i^{v,0} := \{j | v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{valid}\}$;

   $S_i^{v} := \{j | v_i^{j} = v \wedge \sigma_i^{j} \text{valid}\}$;
3. $\texttt{if}\ |S_i^{x_i,0}| \geq n - T \ \wedge\ |S_i^{1-x_i}| = 0\ \texttt{then}\ y_i := x_i$ (I)

   $\texttt{elsif}\ |S_i^0| > |S_i^1|\ \texttt{then}\ y_i := 0\ \texttt{else}\ y_i := 1\ \texttt{fi}.$ (II)

BCEV: Validity for t ≤ T

validity: P_s honest

for P_j honest = $((m,\sigma_s(m)), ?)$

= $(m,\sigma_s(m))$

1. P_s: multisend $(m, \sigma_s(m))$; [receive (x_i, σ_i)]

2. $\forall P_i$: BGP$((x_i, \sigma_i))$; [$\forall P_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]

$$S_i^{v,0} := \{j | v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{valid}\};$$

$$S_i^v := \{j | v_i^j = v \wedge \sigma_i^j \text{valid}\};$$

3. `if` $|S_i^{x_i,0}| \geq n - T \wedge |S_i^{1-x_i}| = 0$ `then` $y_i := x_i$ (I)

`elsif` $|S_i^0| > |S_i^1|$ `then` $y_i := 0$ `else` $y_i := 1$ `fi`. (II)

holds always (for x_i=m)

>

BCEV: Validity for t ≤ T

validity: P_s honest

for P_j honest = ((m,σ_S(m)), ?)

= (m,σ_S(m))

1. P_s: multisend $(m, \sigma_s(m))$; [receive (x_i, σ_i)]

2. $\forall \mathsf{P}_i$: BGP$((x_i, \sigma_i))$; [$\forall \mathsf{P}_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]

$$S_i^{v,0} := \{j | v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{valid}\};$$

$$S_i^{v} := \{j | v_i^{j} = v \wedge \sigma_i^{j} \text{valid}\};$$

holds for t > t_σ (and x_i=m)

3. **if** $|S_i^{x_i,0}| \geq n - T \ \wedge \ |S_i^{1-x_i}| = 0$ **then** $y_i := x_i$ (I)

elsif $|S_i^0| > |S_i^1|$ **then** $y_i := 0$ **else** $y_i := 1$ **fi**. (II)

holds always (for x_i=m)

BCEV: Validity for t ≤ T

validity: P_s honest

secure for $t \leq t_\sigma < n/3$

for P_j honest $= ((m,\sigma_s(m)), ?)$

$= (m,\sigma_s(m))$

1. P_s: multisend $(m, \sigma_s(m))$; [receive (x_i, σ_i)]

2. $\forall \mathsf{P}_i$: BGP$((x_i, \sigma_i))$; [$\forall \mathsf{P}_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]

$$S_i^{v,0} := \{j | v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{valid}\};$$

$$S_i^{v} := \{j | v_i^{j} = v \wedge \sigma_i^{j} \text{valid}\};$$

holds for $t > t_\sigma$ (and $x_i=m$)

3. $\texttt{if } |S_i^{x_i,0}| \geq n - T \ \wedge \ |S_i^{1-x_i}| = 0 \texttt{ then } y_i := x_i$ (I)

$\texttt{elsif } |S_i^0| > |S_i^1| \texttt{ then } y_i := 0 \texttt{ else } y_i := 1 \texttt{ fi.}$ (II)

holds always (for $x_i=m$)

>

BCEV: Validity for $t \leq T$

validity: P_s honest

secure for $t \leq t_\sigma < n/3$

for P_j honest $= ((m,\sigma_s(m)), ?)$

$= (m,\sigma_s(m))$

1. P_s: multisend $(m, \sigma_s(m))$; [receive (x_i, σ_i)]
2. $\forall \mathsf{P}_i$: BGP$((x_i, \sigma_i))$; [$\forall \mathsf{P}_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]

   $S_i^{v,0} := \{j | v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{valid}\}$;

   $S_i^v := \{j | v_i^j = v \wedge \sigma_i^j \text{valid}\}$;

holds for $t > t_\sigma$ (and x_i=m)

3. `if` $|S_i^{x_i,0}| \geq n - T \ \wedge \ |S_i^{1-x_i}| = 0$ `then` $y_i := x_i$ (I)

   `elsif` $|S_i^0| > |S_i^1|$ `then` $y_i := 0$ `else` $y_i := 1$ `fi`. (II)

holds always (for x_i=m)

holds for $t \leq t_\sigma$ (and m=0)

>

BCEV: Consistency for $t \leq t_\sigma$

1. P_s: multisend $(m, \sigma_s(m))$; [receive (x_i, σ_i)]
2. $\forall \mathsf{P}_i$: BGP$((x_i, \sigma_i))$; [$\forall \mathsf{P}_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]

   $S_i^{v,0} := \{j | v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{valid}\}$;

   $S_i^v := \{j | v_i^j = v \wedge \sigma_i^j \text{valid}\}$;
3. `if` $|S_i^{x_i,0}| \geq n - T \wedge |S_i^{1-x_i}| = 0$ `then` $y_i := x_i$ (I)

   `elsif` $|S_i^0| > |S_i^1|$ `then` $y_i := 0$ `else` $y_i := 1$ `fi`. (II)

BCEV: Consistency for $t \leq t_\sigma$

secure for
$t \leq t_\sigma < n/3$

1. P_s: multisend $(m, \sigma_s(m))$; [receive (x_i, σ_i)]
2. $\forall \mathsf{P}_i$: $\mathrm{BGP}((x_i, \sigma_i))$; [$\forall \mathsf{P}_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]

   $S_i^{v,0} := \{j | v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{valid}\};$

   $S_i^{v} := \{j | v_i^{j} = v \wedge \sigma_i^{j} \text{valid}\};$

3. $\texttt{if } |S_i^{x_i,0}| \geq n - T \ \wedge \ |S_i^{1-x_i}| = 0 \texttt{ then } y_i := x_i$ (I)

   $\texttt{elsif } |S_i^0| > |S_i^1| \texttt{ then } y_i := 0 \texttt{ else } y_i := 1 \texttt{ fi.}$ (II)

BCEV: Consistency for $t \leq t_\sigma$

secure for $t \leq t_\sigma < n/3$

1. P_s: multisend $(m, \sigma_s(m))$; [receive (x_i, σ_i)]
2. $\forall \mathsf{P}_i$: BGP$((x_i, \sigma_i))$; [$\forall \mathsf{P}_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]

   $S_i^{v,0} := \{j | v_i^{j,0} = v \wedge \sigma_i^{j,0}\text{valid}\};$

   $S_i^v := \{j | v_i^j = v \wedge \sigma_i^j\text{valid}\};$

   $S_i^v = S_j^v$

3. $\texttt{if } |S_i^{x_i,0}| \geq n - T \;\wedge\; |S_i^{1-x_i}| = 0 \texttt{ then } y_i := x_i$ (I)

   $\texttt{elsif } |S_i^0| > |S_i^1| \texttt{ then } y_i := 0 \texttt{ else } y_i := 1 \texttt{ fi.}$ (II)

BCEV: Consistency for $t \leq t_\sigma$

secure for
$t \leq t_\sigma < n/3$

1. P_s: multisend $(m, \sigma_s(m))$; [receive (x_i, σ_i)]
2. $\forall \mathsf{P}_i$: BGP$((x_i, \sigma_i))$; [$\forall \mathsf{P}_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]

   $S_i^{v,0} := \{j | v_i^{j,0} = v \wedge \sigma_i^{j,0}\text{valid}\}$;

   $S_i^{v} := \{j | v_i^{j} = v \wedge \sigma_i^{j}\text{valid}\}$;

   $S_i^v = S_j^v$

3. $\texttt{if } |S_i^{x_i,0}| \geq n - T \ \wedge \ |S_i^{1-x_i}| = 0 \texttt{ then } y_i := x_i$ (I)

   $\texttt{elsif } |S_i^0| > |S_i^1| \texttt{ then } y_i := 0 \texttt{ else } y_i := 1 \texttt{ fi.}$ (II)

all decisions
here identical

>

BCEV: Consistency for $t \leq t_\sigma$

secure for $t \leq t_\sigma < n/3$

1. P_s: multisend $(m, \sigma_s(m))$; [receive (x_i, σ_i)]
2. $\forall P_i$: $\mathrm{BGP}((x_i, \sigma_i))$; [$\forall P_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]

   $S_i^{v,0} := \{j | v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{valid}\}$;

   $S_i^v := \{j | v_i^j = v \wedge \sigma_i^j \text{valid}\}$;

$S_i^v = S_j^v$

identical S_j^v

3. $\texttt{if } |S_i^{x_i,0}| \geq n - T \wedge |S_i^{1-x_i}| = 0 \texttt{ then } y_i := x_i$ (I)

   $\texttt{elsif } |S_i^0| > |S_i^1| \texttt{ then } y_i := 0 \texttt{ else } y_i := 1 \texttt{ fi.}$ (II)

all decisions here identical

>

BCEV: Consistency for $t \leq t_\sigma$

secure for $t \leq t_\sigma < n/3$

$j \in S_i^{v,0} \Leftrightarrow j \in S_i^v$ for P_j honest

1. P_s: multisend $(m, \sigma_s(m))$; [receive (x_i, σ_i)]
2. $\forall P_i$: BGP$((x_i, \sigma_i))$; [$\forall P_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]

   $S_i^{v,0} := \{j | v_i^{j,0} = v \wedge \sigma_i^{j,0}\text{valid}\}$;

   $S_i^v := \{j | v_i^j = v \wedge \sigma_i^j\text{valid}\}$;

$S_i^v = S_j^v$

identical S_j^v

3. `if` $|S_i^{x_i,0}| \geq n - T \wedge |S_i^{1-x_i}| = 0$ `then` $y_i := x_i$ (I)

   `elsif` $|S_i^0| > |S_i^1|$ `then` $y_i := 0$ `else` $y_i := 1$ `fi`. (II)

all decisions here identical

Hybrid Broadcast (HBC)

- For $2t_\sigma + T < n$ and $t_p = 0$ HBC achieves
  - For $t = 0$ full BC
  - For $t \leq t_\sigma$ full BC, conditional on PKI consistency
  - For $t \leq T$ full BC, conditional on unforgeability and PKI consistency
- Protocol idea:
  - Attempt detectable precomputation of a new PKI [FHHW03]; fall back to existing PKI
  - Run an HBC for $2t_\sigma + T < n$ and $t_p = -1$ constructed from BCEV and DS

Hybrid Broadcast (HBC) for $t_p = -1$

1. P_s: DS(m); [receive d_i]
2. P_s: BCEV(m); [receive b_i]
3. Multisend $(b_i, \sigma_i(b_i))$; [$\forall \mathsf{P}_j$ receive (c_i^j, σ_i^j)]
   $M_i^v := \{\sigma_i^j | c_i^j = v \wedge \sigma_i^j \text{valid}\}$;
4. `if` $\exists\, v : |M_i^v| \geq n - t_\sigma$ `then` DS(M_i^v)
   and $y_i := v$; [receive S_i^j] (I)
   `else` DS($\emptyset$); [receive S_i^j]
   `If` $\exists\, v$ and a set S_i^j of valid signatures on v
   and $|S_i^j| \geq n - t_\sigma$ `then` $y_i := v$; (II)
   `else` $y_i := d_i$; (III)
   `fi`
   `fi`

>

HBC: Security for t ≤ t_σ

1. P_s: DS(m); [receive d_i]
2. P_s: BCEV(m); [receive b_i]
3. Multisend $(b_i, \sigma_i(b_i))$; [$\forall \mathsf{P}_j$ receive (c_i^j, σ_i^j)]

   $M_i^v := \{\sigma_i^j | c_i^j = v \wedge \sigma_i^j \text{valid}\}$;
4. `if` $\exists\ v\ :\ |M_i^v| \geq n - t_\sigma$ `then` DS(M_i^v)

   and $y_i := v$; [receive S_i^j] (I)

   `else` DS($\emptyset$); [receive S_i^j]

   `If` $\exists\ v$ and a set S_i^j of valid signatures on v

   and $|S_i^j| \geq n - t_\sigma$ `then` $y_i := v$; (II)

   `else` $y_i := d_i$; (III)

   `fi`

   `fi`

>

HBC: Security for t ≤ t_σ

BC for t ≤ t_σ

1. P_s: $\mathrm{DS}(m)$; [receive d_i]
2. P_s: $\mathrm{BCEV}(m)$; [receive b_i]
3. Multisend $(b_i, \sigma_i(b_i))$; [$\forall \mathsf{P}_j$ receive (c_i^j, σ_i^j)]

   $M_i^v := \{\sigma_i^j | c_i^j = v \wedge \sigma_i^j \text{valid}\}$;

4. `if` $\exists\, v : |M_i^v| \geq n - t_\sigma$ `then` $\mathrm{DS}(M_i^v)$

   and $y_i := v$; [receive S_i^j] (I)

   `else` $\mathrm{DS}(\emptyset)$; [receive S_i^j]

   `If` $\exists\, v$ and a set S_i^j of valid signatures on v

   and $|S_i^j| \geq n - t_\sigma$ `then` $y_i := v$; (II)

   `else` $y_i := d_i$; (III)

   `fi`

   `fi`

HBC: Security for t ≤ t_σ

BC for t ≤ t_σ

holds for t ≤ t_σ

1. P_s: $DS(m)$; [receive d_i]
2. P_s: $BCEV(m)$; [receive b_i]
3. Multisend $(b_i, \sigma_i(b_i))$; [$\forall P_j$ receive (c_i^j, σ_i^j)]

   $M_i^v := \{\sigma_i^j \mid c_i^j = v \wedge \sigma_i^j \text{valid}\}$;
4. `if` $\exists\, v : |M_i^v| \geq n - t_\sigma$ `then` $DS(M_i^v)$

   and $y_i := v$; [receive S_i^j] (I)

   `else` $DS(\emptyset)$; [receive S_i^j]

   `If` $\exists\, v$ and a set S_i^j of valid signatures on v

   and $|S_i^j| \geq n - t_\sigma$ `then` $y_i := v$; (II)

   `else` $y_i := d_i$; (III)

   `fi`

   `fi`

HBC: Consistency for $t_\sigma < t \leq T$

1. P_s: $\mathrm{DS}(m)$; [receive d_i]
2. P_s: $\mathrm{BCEV}(m)$; [receive b_i]
3. Multisend $(b_i, \sigma_i(b_i))$; [$\forall \mathsf{P}_j$ receive (c_i^j, σ_i^j)]
   $M_i^v := \{\sigma_i^j | c_i^j = v \wedge \sigma_i^j \text{valid}\}$;
4. `if` $\exists\, v : |M_i^v| \geq n - t_\sigma$ `then` $\mathrm{DS}(M_i^v)$
   and $y_i := v$; [receive S_i^j] (I)
   `else` $\mathrm{DS}(\emptyset)$; [receive S_i^j]
   `If` $\exists\, v$ and a set S_i^j of valid signatures on v
   and $|S_i^j| \geq n - t_\sigma$ `then` $y_i := v$; (II)
   `else` $y_i := d_i$; (III)
   `fi`
   `fi`

HBC: Consistency for $t_\sigma < t \leq T$

BC for t > t_σ

1. P_s: $\mathrm{DS}(m)$; [receive d_i]
2. P_s: $\mathrm{BCEV}(m)$; [receive b_i]
3. Multisend $(b_i, \sigma_i(b_i))$; [$\forall \mathsf{P}_j$ receive (c_i^j, σ_i^j)]
   $M_i^v := \{\sigma_i^j | c_i^j = v \wedge \sigma_i^j \text{valid}\}$;
4. `if` $\exists\, v : |M_i^v| \geq n - t_\sigma$ `then` $\mathrm{DS}(M_i^v)$
   and $y_i := v$; [receive S_i^j] (I)
   `else` $\mathrm{DS}(\emptyset)$; [receive S_i^j]
   `If` $\exists\, v$ and a set S_i^j of valid signatures on v
   and $|S_i^j| \geq n - t_\sigma$ `then` $y_i := v$; (II)
   `else` $y_i := d_i$; (III)
   `fi`
   `fi`

>

HBC: Consistency for $t_\sigma < t \leq T$

1. P_s: $\mathrm{DS}(m)$; [receive d_i]

   BC for $t > t_\sigma$

2. P_s: $\mathrm{BCEV}(m)$; [receive b_i]
3. Multisend $(b_i, \sigma_i(b_i))$; [$\forall \mathsf{P}_j$ receive (c_i^j, σ_i^j)]

   $M_i^v := \{\sigma_i^j | c_i^j = v \wedge \sigma_i^j \text{valid}\}$;

4. `if` $\exists\ v\ :\ |M_i^v| \geq n - t_\sigma$ `then` $\mathrm{DS}(M_i^v)$

   and $y_i := v$; [receive S_i^j] (I)

   `else` $\mathrm{DS}(\emptyset)$; [receive S_i^j]

   consistent for $t > t_\sigma$

   `If` $\exists\ v$ and a set S_i^j of valid signatures on v

   and $|S_i^j| \geq n - t_\sigma$ `then` $y_i := v$; (II)

   `else` $y_i := d_i$; (III)

   `fi`

   `fi`

>

HBC: Consistency for $t_\sigma < t \leq T$

1. P_s: DS(m); [receive d_i]
2. P_s: BCEV(m); [receive b_i]
3. Multisend $(b_i, \sigma_i(b_i))$; [$\forall P_j$ receive (c_i^j, σ_i^j)]

   $M_i^v := \{\sigma_i^j | c_i^j = v \wedge \sigma_i^j \text{valid}\}$;
4. `if` $\exists\, v : |M_i^v| \geq n - t_\sigma$ `then` DS(M_i^v)

   and $y_i := v$; [receive S_i^j] (I)

   `else` DS($\emptyset$); [receive S_i^j]

   `If` $\exists\, v$ and a set S_i^j of valid signatures on v

   and $|S_i^j| \geq n - t_\sigma$ `then` $y_i := v$; (II)

   `else` $y_i := d_i$; (III)

   `fi`

   `fi`

BC for $t > t_\sigma$

if holds then ...

consistent for $t > t_\sigma$

>

HBC: Consistency for $t_\sigma < t \leq T$

1. P_s: $\mathrm{DS}(m)$; [receive d_i]
2. P_s: $\mathrm{BCEV}(m)$; [receive b_i]
3. Multisend $(b_i, \sigma_i(b_i))$; [$\forall P_j$ receive (c_i^j, σ_i^j)]
   $M_i^v := \{\sigma_i^j | c_i^j = v \wedge \sigma_i^j \text{valid}\}$;
4. `if` $\exists\, v \;:\; |M_i^v| \geq n - t_\sigma$ `then` $\mathrm{DS}(M_i^v)$
   and $y_i := v$; [receive S_i^j] (I)
   `else` $\mathrm{DS}(\emptyset)$; [receive S_i^j]
   `If` $\exists\, v$ and a set S_i^j of valid signatures on v
   and $|S_i^j| \geq n - t_\sigma$ `then` $y_i := v$; (II)
   `else` $y_i := d_i$; (III)
   `fi`
   `fi`

BC for $t > t_\sigma$

if holds then ...

consistent for $t > t_\sigma$

also holds for same v

>

HBC: Validity for $t_\sigma < t \leq T$

1. P_s: $\mathrm{DS}(m)$; [receive d_i]
2. P_s: $\mathrm{BCEV}(m)$; [receive b_i]
3. Multisend $(b_i, \sigma_i(b_i))$; [$\forall \mathsf{P}_j$ receive (c_i^j, σ_i^j)]
   $M_i^v := \{\sigma_i^j | c_i^j = v \wedge \sigma_i^j \text{valid}\}$;
4. `if` $\exists\ v\ :\ |M_i^v| \geq n - t_\sigma$ `then` $\mathrm{DS}(M_i^v)$
   and $y_i := v$; [receive S_i^j] (I)
   `else` $\mathrm{DS}(\emptyset)$; [receive S_i^j]
   `If` $\exists\ v$ and a set S_i^j of valid signatures on v
   and $|S_i^j| \geq n - t_\sigma$ `then` $y_i := v$; (II)
   `else` $y_i := d_i$; (III)
   `fi`
   `fi`

>

HBC: Validity for $t_\sigma < t \leq T$

BC for $t > t_\sigma$

guarantees validity

1. P_s: $\mathrm{DS}(m)$; $\quad$ [receive d_i]
2. P_s: $\mathrm{BCEV}(m)$; $\quad$ [receive b_i]
3. Multisend $(b_i, \sigma_i(b_i))$; $\quad$ [$\forall \mathsf{P}_j$ receive (c_i^j, σ_i^j)]

   $M_i^v := \{\sigma_i^j \mid c_i^j = v \wedge \sigma_i^j \text{valid}\}$;
4. `if` $\exists\, v : |M_i^v| \geq n - t_\sigma$ `then` $\mathrm{DS}(M_i^v)$

   and $y_i := v$; $\quad$ [receive S_i^j] $\quad$ (I)

   `else` $\mathrm{DS}(\emptyset)$; $\quad$ [receive S_i^j]

   `If` $\exists\, v$ and a set S_i^j of valid signatures on v

   and $|S_i^j| \geq n - t_\sigma$ `then` $y_i := v$; $\quad$ (II)

   `else` $y_i := d_i$; $\quad$ (III)

   `fi`

   `fi`

>

HBC: Validity for $t_\sigma < t \leq T$

1. P_s: $\mathrm{DS}(m)$; $\quad$ [receive d_i]

BC for $t > t_\sigma$

2. P_s: $\mathrm{BCEV}(m)$; $\quad$ [receive b_i]

guarantees validity

3. Multisend $(b_i, \sigma_i(b_i))$; $\quad$ [$\forall \mathsf{P}_j$ receive (c_i^j, σ_i^j)]

$M_i^v := \{\sigma_i^j | c_i^j = v \wedge \sigma_i^j \text{valid}\}$;

can only hold for v = m

4. $\texttt{if}$ $\quad \exists\, v \ : \ |M_i^v| \geq n - t_\sigma$ $\texttt{then}$ $\mathrm{DS}(M_i^v)$

and $y_i := v$; $\quad$ [receive S_i^j] $\quad$ (I)

$\texttt{else}$ $\quad \mathrm{DS}(\emptyset)$; $\quad$ [receive S_i^j]

$\texttt{If}$ $\exists\, v$ and a set S_i^j of valid signatures on v

and $|S_i^j| \geq n - t_\sigma$ $\texttt{then}$ $y_i := v$; $\quad$ (II)

$\texttt{else}$ $y_i := d_i$; $\quad$ (III)

$\texttt{fi}$

$\texttt{fi}$

HBC: Validity for $t_\sigma < t \leq T$

1. P_s: $\mathrm{DS}(m)$; [receive d_i]
2. P_s: $\mathrm{BCEV}(m)$; [receive b_i]
3. Multisend $(b_i, \sigma_i(b_i))$; [$\forall P_j$ receive (c_i^j, σ_i^j)]
   $M_i^v := \{\sigma_i^j | c_i^j = v \wedge \sigma_i^j \text{valid}\}$;
4. **if** $\exists\, v : |M_i^v| \geq n - t_\sigma$ **then** $\mathrm{DS}(M_i^v)$
   and $y_i := v$; [receive S_i^j] (I)
   else $\mathrm{DS}(\emptyset)$; [receive S_i^j]
   If $\exists\, v$ and a set S_i^j of valid signatures on v
   and $|S_i^j| \geq n - t_\sigma$ **then** $y_i := v$; (II)
   else $y_i := d_i$; (III)
   fi
   fi

BC for $t > t_\sigma$

guarantees validity

can only hold for v = m

can only hold for v = m

>

HBC: Validity for $t_\sigma < t \leq T$

1. P_s: $\mathrm{DS}(m)$; — BC for $t > t_\sigma$ — [receive d_i]
2. P_s: $\mathrm{BCEV}(m)$; — guarantees validity — [receive b_i]
3. Multisend $(b_i, \sigma_i(b_i))$; [$\forall P_j$ receive (c_i^j, σ_i^j)]

   $M_i^v := \{\sigma_i^j | c_i^j = v \wedge \sigma_i^j \text{valid}\}$; — can only hold for v = m

4. **if** $\exists\ v\ :\ |M_i^v| \geq n - t_\sigma$ **then** $\mathrm{DS}(M_i^v)$
   and $y_i := v$; [receive S_i^j] (I)

   else $\mathrm{DS}(\emptyset)$; [receive S_i^j]

   If $\exists\ v$ and a set S_i^j of valid signatures on v
   and $|S_i^j| \geq n - t_\sigma$ **then** $y_i := v$; (II)

   else $y_i := d_i$; (III)

   fi

   fi

$d_i = m$

can only hold for v = m

>