

Optimally Hybrid-Secure MPC

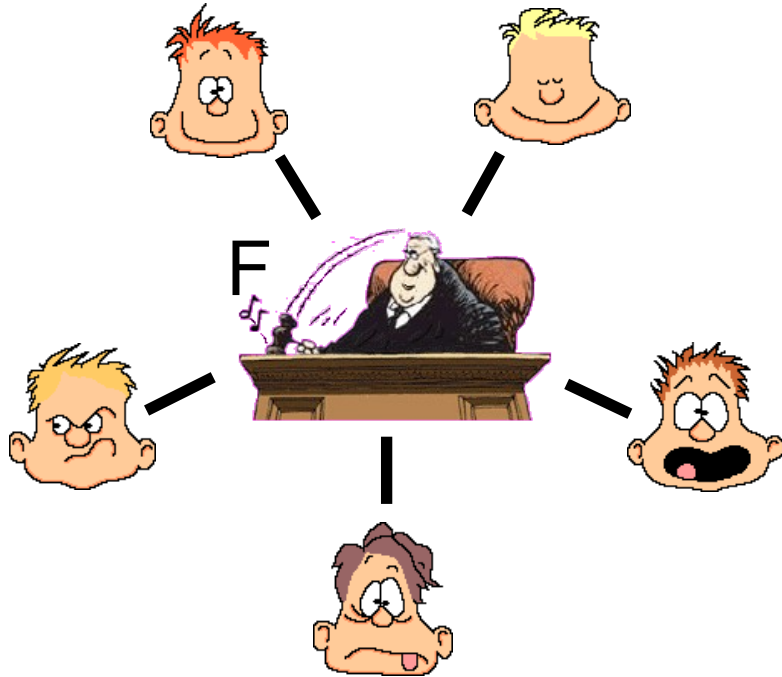
Dominik Raub

Institute of Theoretical Computer Science
ETH Zürich

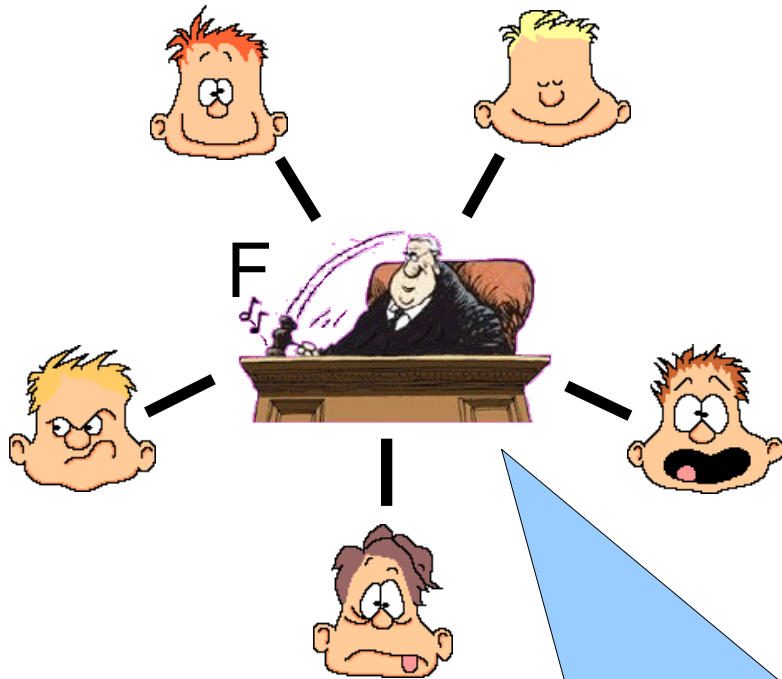
on joint work with
M. Fitzi, C. Lucas, U. Maurer

Tartu, 2009/10/05

Multi-Party Computation (MPC)

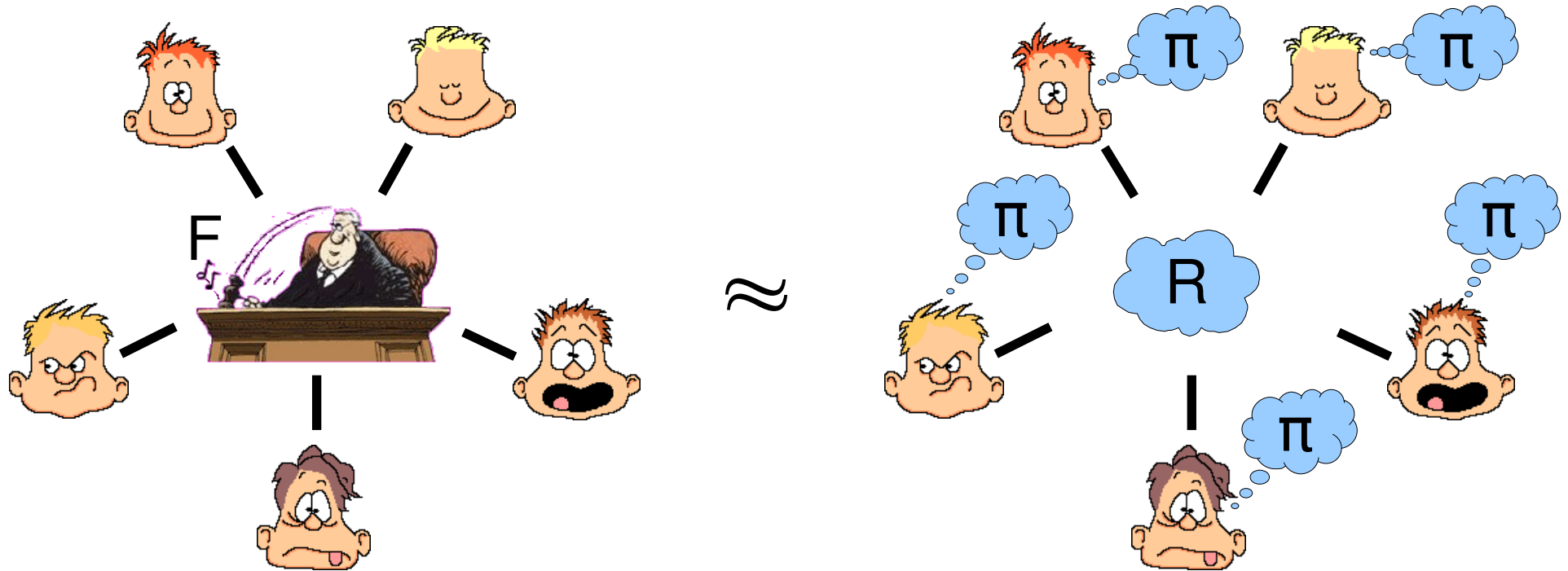


Multi-Party Computation (MPC)

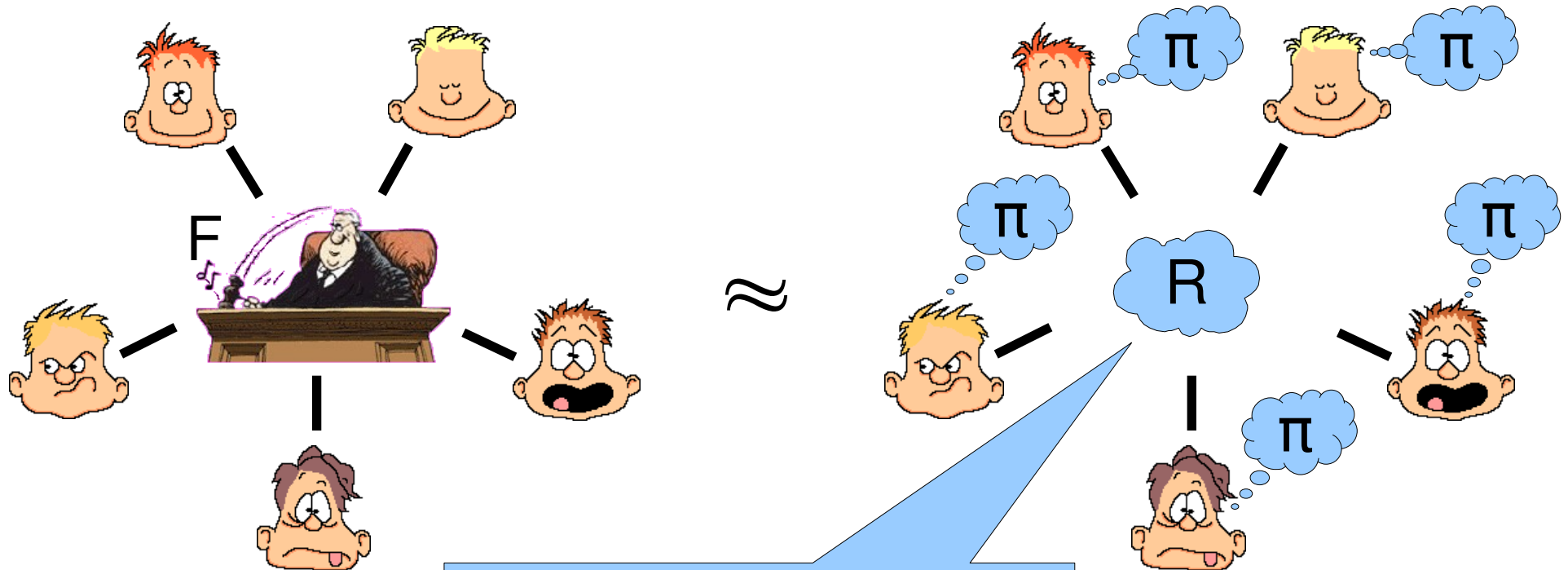


- Voting
 - Auctions
 - Who is richest?
- ⇒ privacy, correctness required

Multi-Party Computation (MPC)



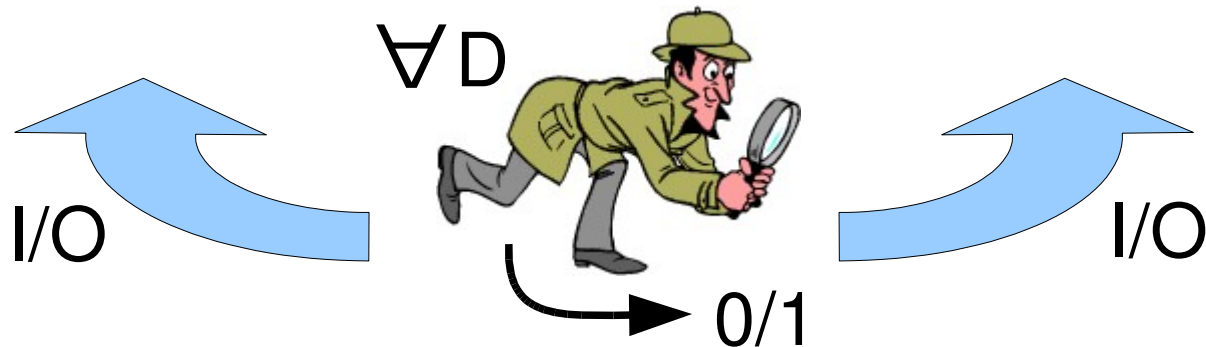
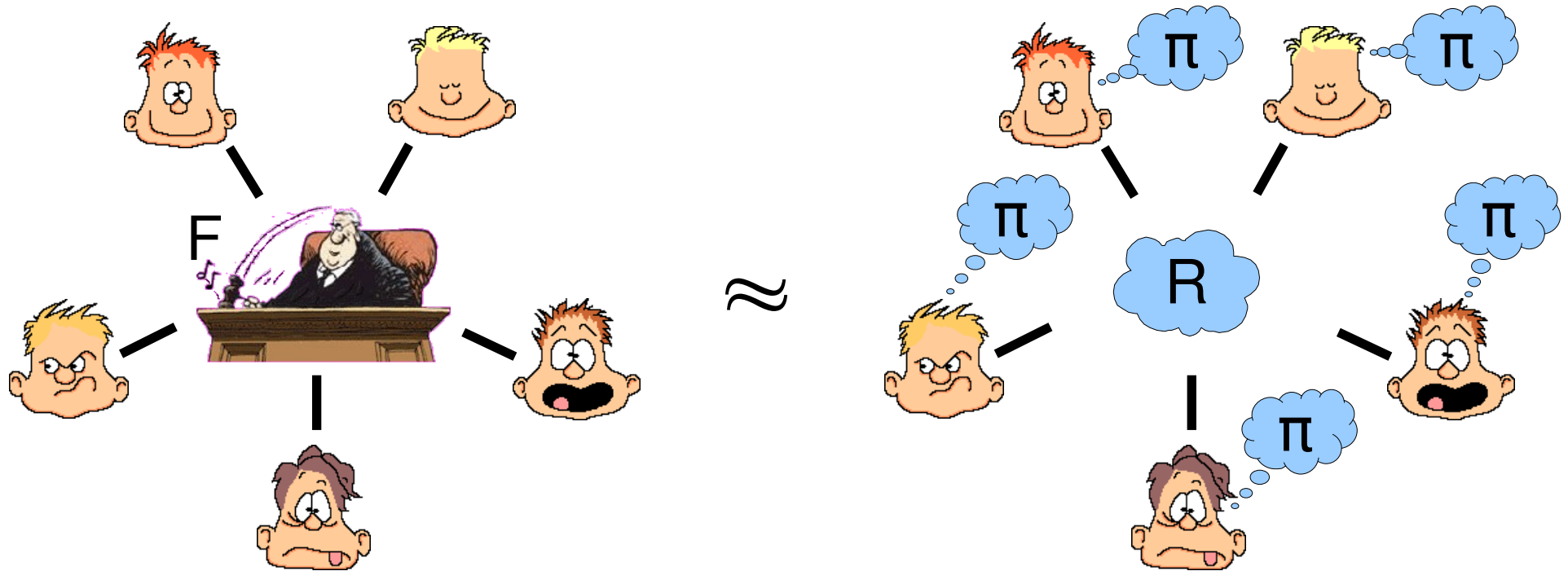
Multi-Party Computation (MPC)



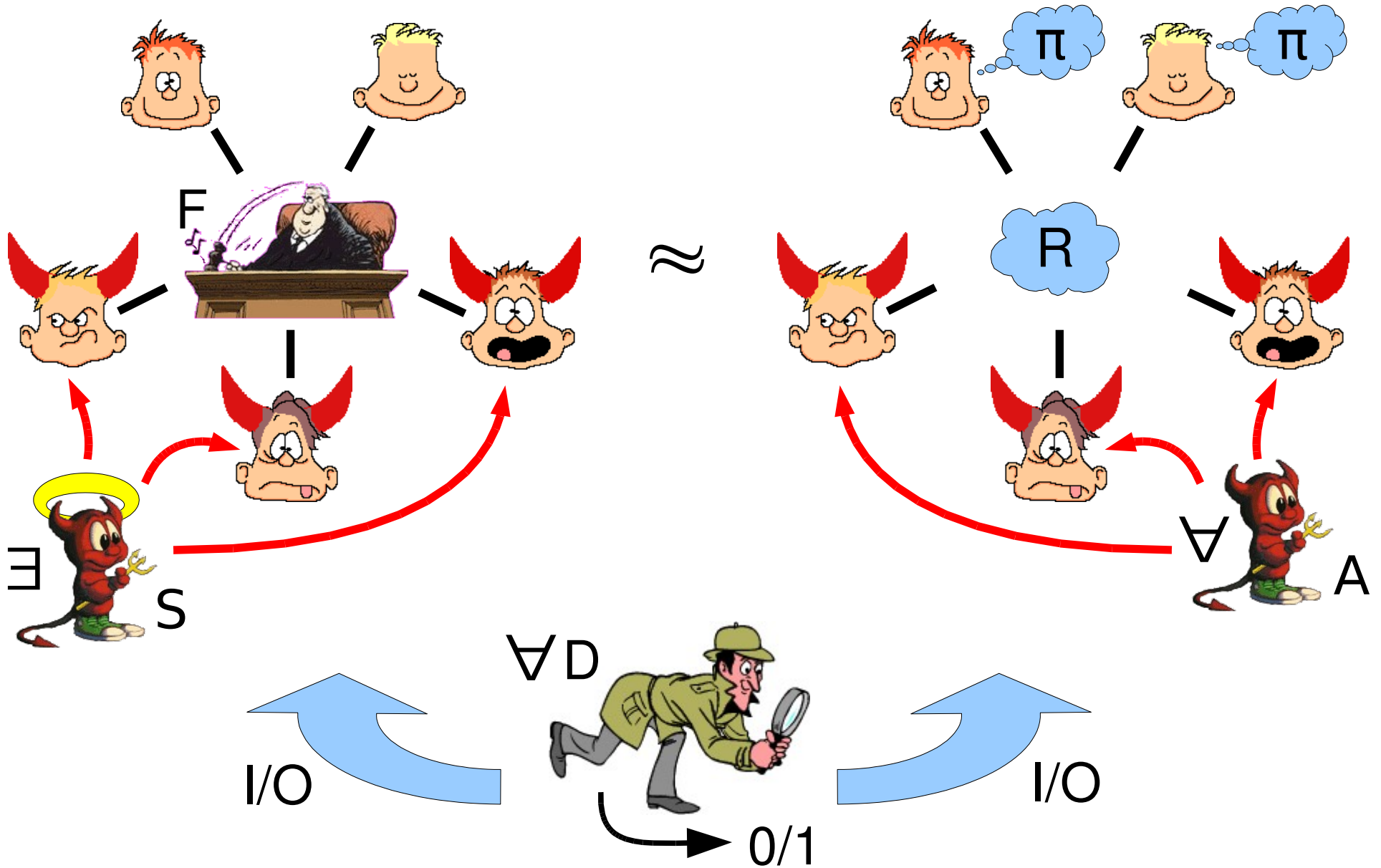
Generally encompasses:

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

Multi-Party Computation (MPC)



Multi-Party Computation (MPC)



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]
- We cannot have IT full security always
 - ⇒ Trade-offs to be made
 - ⇒ Graceful degradation desired
- ⇒ Hybrid Multi-Party Computation (HMPC)

Hybrid MPC (HMPC)

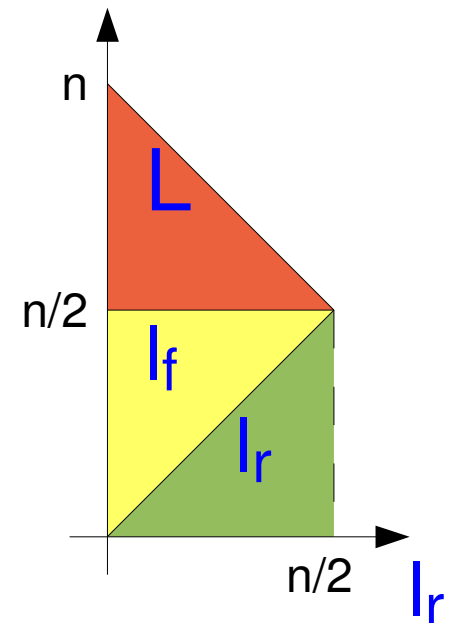
- Different guarantees depending on t :
 - For $t \leq l_r$ full (robust) security
 - For $t \leq l_f$ fair security
 - For $t \leq L$ abort security
 - While tolerating:
 - For $t \leq t_c$ computationally unbounded adversaries
 - For $t \leq t_\sigma$ signature forgery
 - For $t \leq t_p$ inconsistent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

Limitations for HMPC with BC

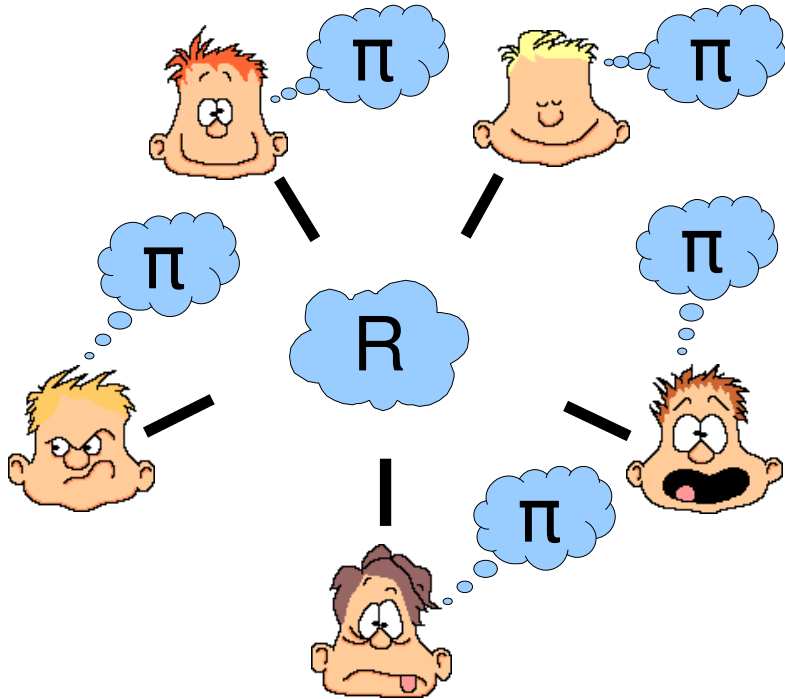
- IT security for $t \leq t_c$ only if $t_c < n/2$ [Kil00]
- Fair security for $t \leq l_f$ only if $l_f < n/2$ [Cle86]
- Full security for $t \leq l_r$ and abort security for $t \leq L$ only if $l_r + L < n$ [IKLP06], [Kat07]

- Therefore:

$$\begin{aligned} t_c < n/2 \quad \wedge \quad l_r \leq l_f \leq L \\ \wedge \quad l_f < n/2 \quad \wedge \quad l_r + L < n \end{aligned} \quad (1)$$



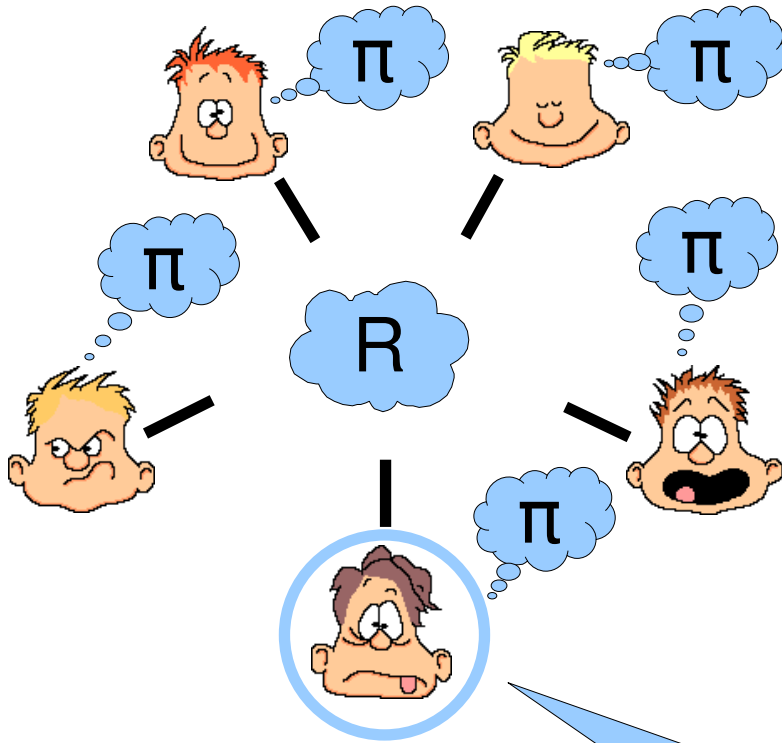
Optimal Hybrid MPC (with BC)



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)

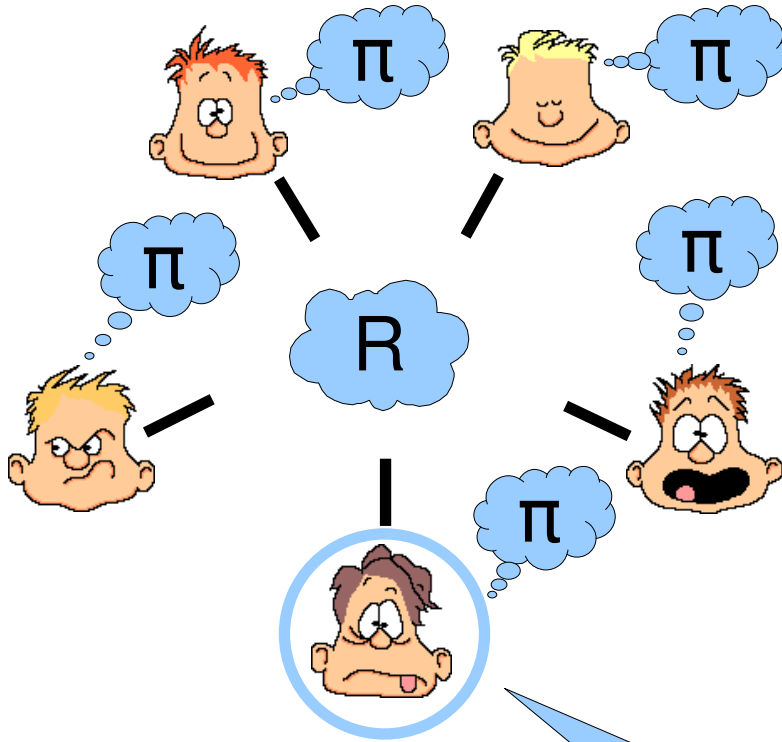


Goal: For any $\rho < n/2$

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

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

Optimal Hybrid MPC (with BC)

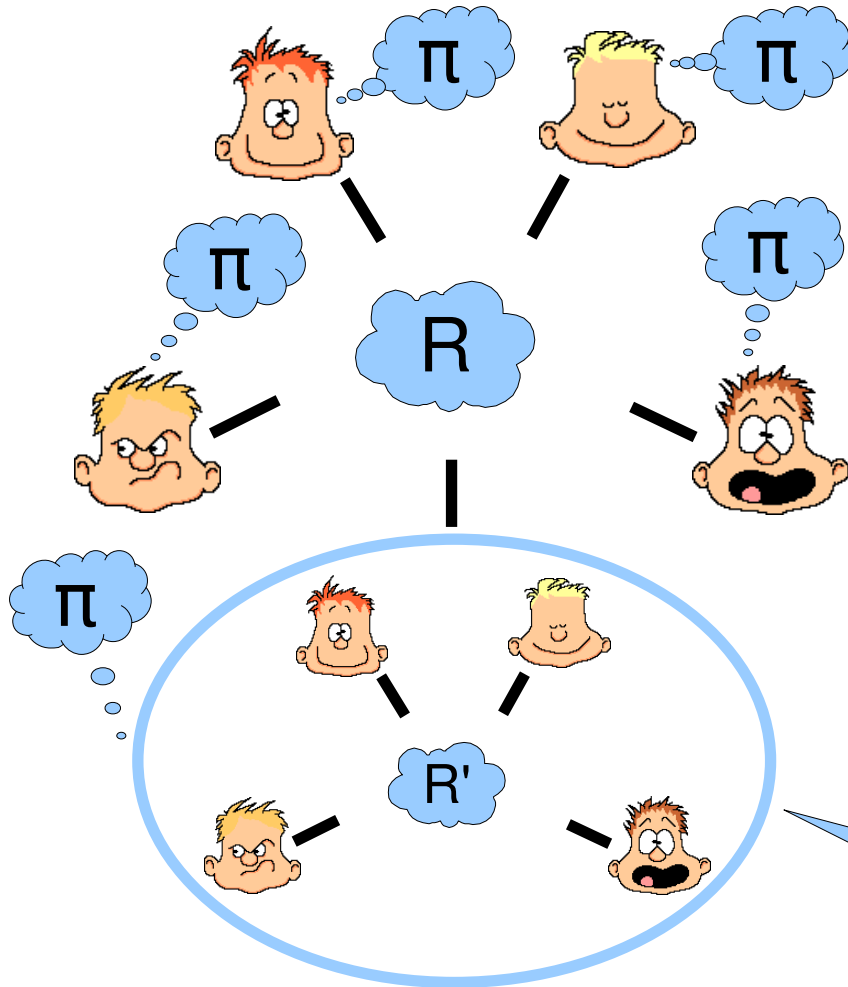


Goal: For any $\rho < n/2$

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

Trusted \Rightarrow
IT fairness, correctness

Optimal Hybrid MPC (with BC)



[Cha89]: emulate!

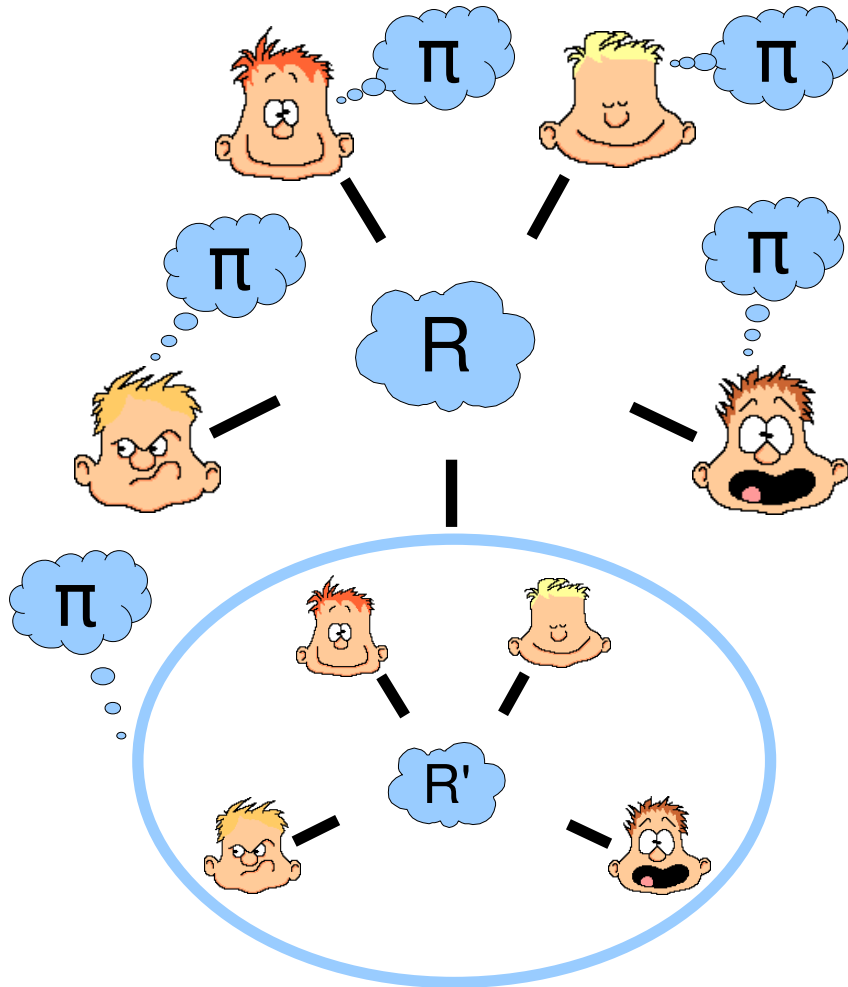
\Rightarrow honest for $t < n/2$ [RB89]

$\Rightarrow t < n/2$: IT fair, correct

$\Rightarrow t \geq n/2$: CO private, correct

Trusted \Rightarrow
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

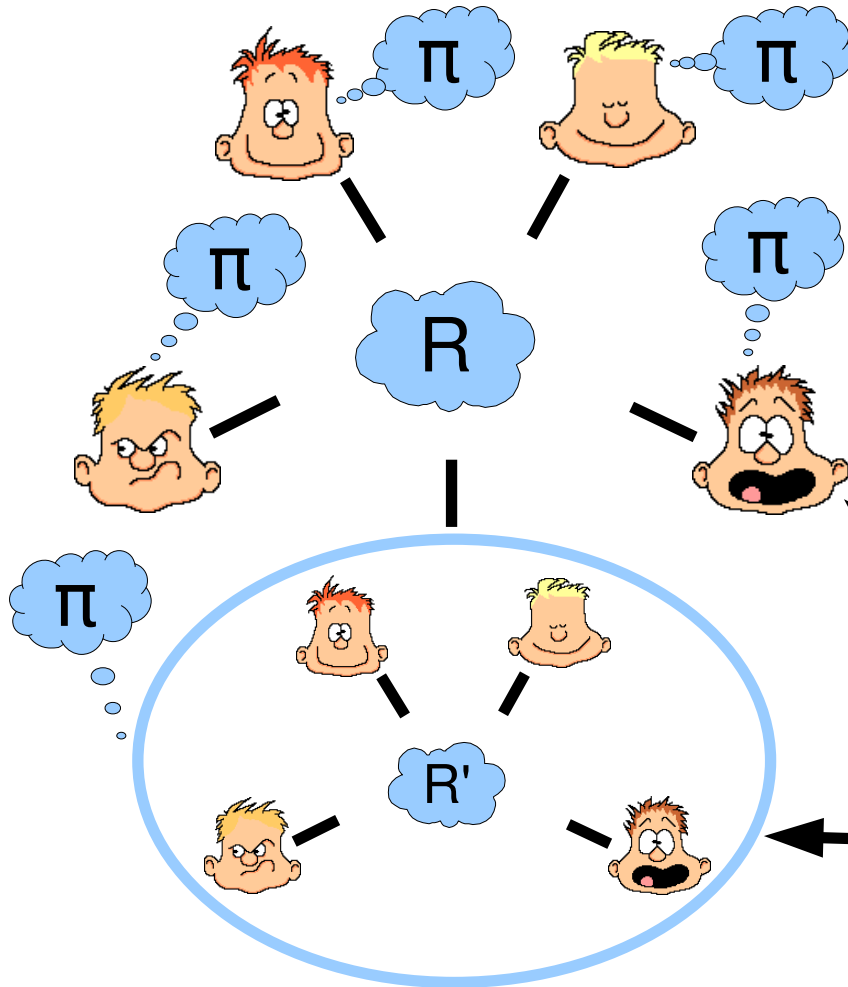
Use sharing qualifying all sets of emulated and $n-\rho$ actual parties

⇒ $t \leq \rho$: IT robust, correct

⇒ $t < n/2$: IT fair, correct

⇒ $t < n-\rho$: CO private, correct

Optimal Hybrid MPC (with BC)



Share inputs

$\Rightarrow t < n/2$: IT privacy

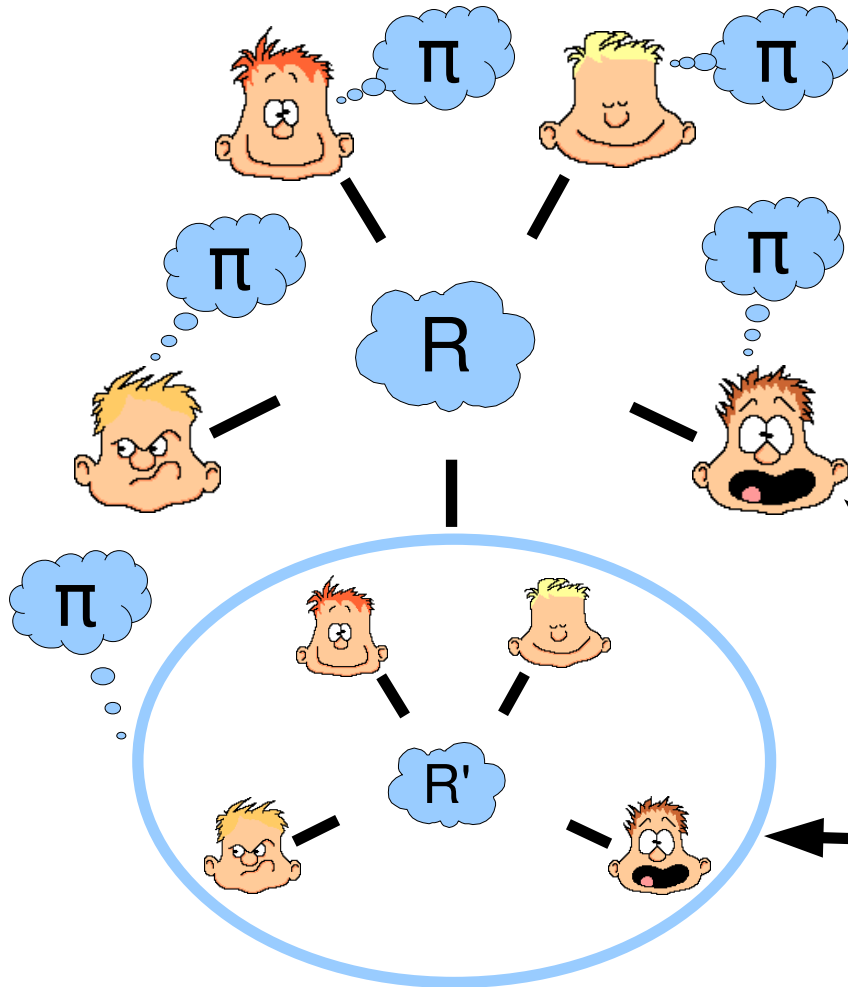
$\Rightarrow t \geq n/2$: no correctness

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

(x_i^{des})

(x_i^{em})

Optimal Hybrid MPC (with BC)



Share and commit

⇒ no robustness or

⇒ no correctness for $t \geq n/2$

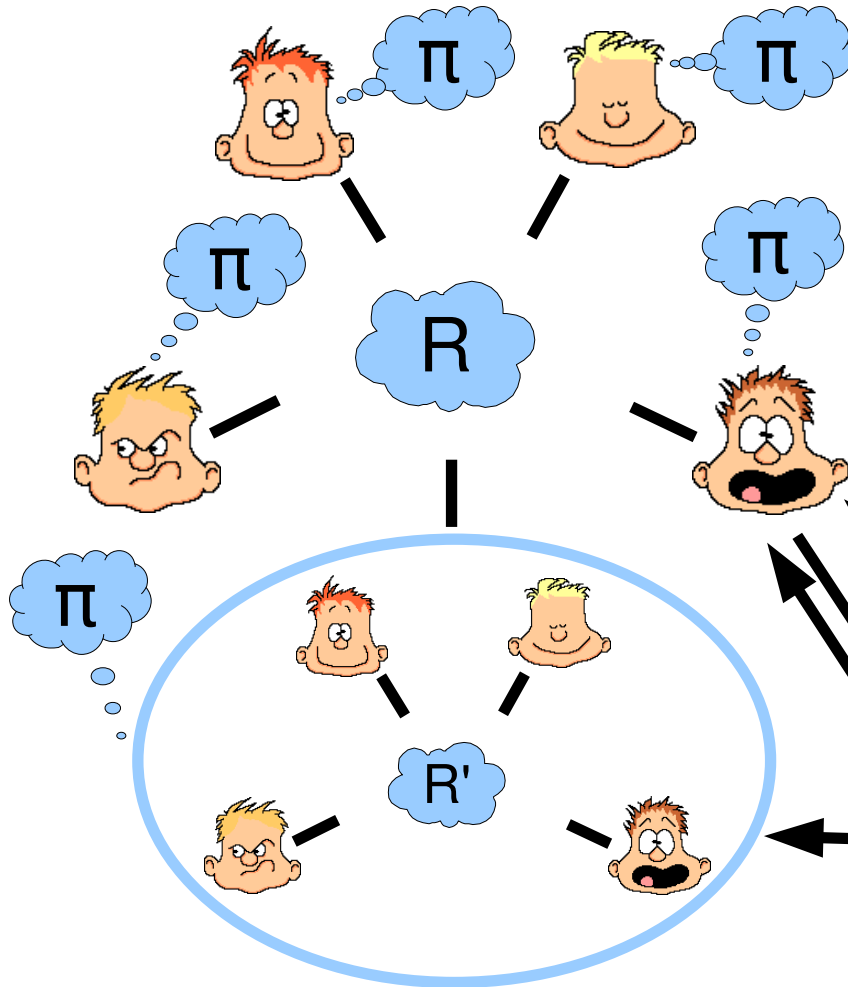
$$x_i = x_i^{\text{des}} \oplus x_i^{\text{em}}$$

$$(c_i, o_i) = \text{com}_H(x_i^{\text{em}})$$

$$(x_i^{\text{des}}, c_i)$$

$$(x_i^{\text{em}}, o_i)$$

Optimal Hybrid MPC (with BC)



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

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

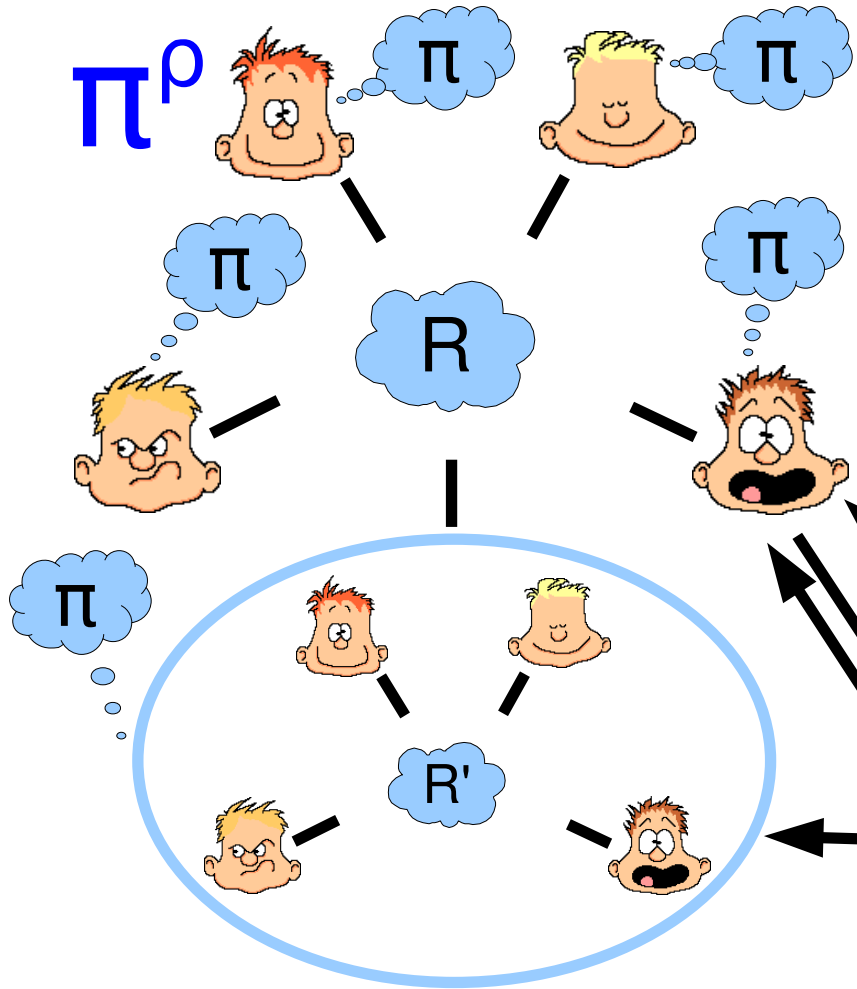
$$(c_i, o_i) = \text{com}_H(x_i^{\text{em}})$$

$$(x_i^{\text{des}}, c_i)$$

$$(x_i^{\text{em}}, o_i)$$

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

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

$$(c_i, o_i) = \text{com}_H(x_i^{\text{em}})$$

$$(x_i^{\text{des}}, c_i)$$

$$(x_i^{\text{em}}, o_i)$$

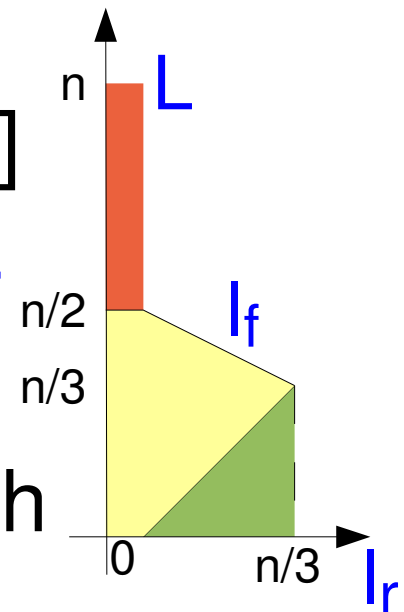
complaint? input x_i

Hybrid MPC without BC or PKI

- Fair security for $t \leq l_f$ only if $l_f < n/2$ [Cle86]
- IT security for $t \leq t_c$ only if $t_c < n/2$ [Kil00]
- Full security for $t \leq l_r$ and abort security for $t \leq L$ only if $l_r > 0 \Rightarrow l_r + 2L < n$ [FHHW03]
- Protocol π^p with the BC from [FHHW03] achieves bound

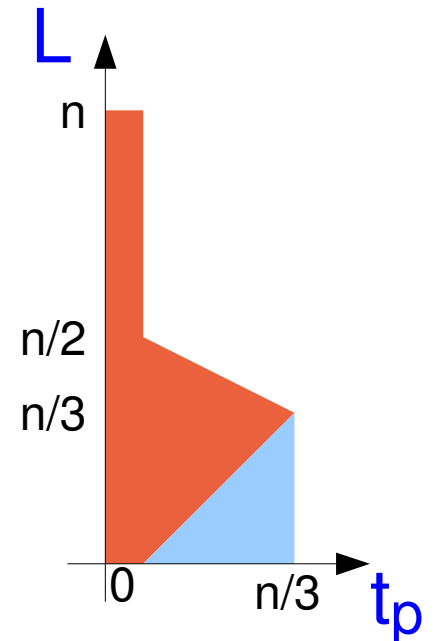
$$t_c < n/2 \wedge l_r \leq l_f \leq L$$

$$\wedge l_f < n/2 \wedge (l_r > 0 \Rightarrow l_r + 2L < n) \quad (2)$$
- Improves over [FHHW03] for $p=0$, 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

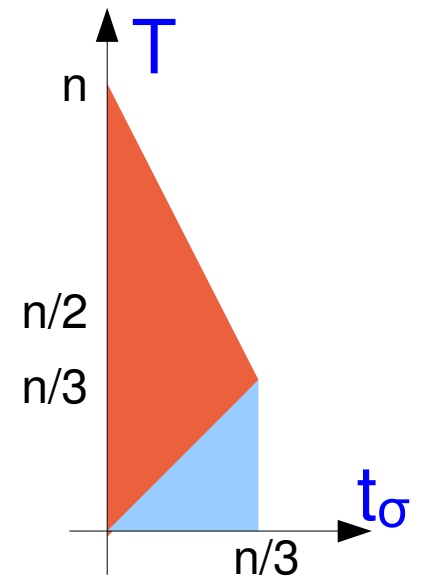
$$t_c < n/2 \quad \wedge \quad l_r \leq l_f \leq L \quad \wedge \quad l_f < n/2 \quad \wedge \quad l_r + L < n$$

$$\wedge \quad 2t_\sigma + L < n \quad \wedge \quad (t_p > 0 \Rightarrow t_p + 2L < n) \quad (3)$$

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

Hybrid MPC without BC, with PKI

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

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

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

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

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

BCEV: Validity for $t \leq T$

1. P_s : `multisend` ($m, \sigma_s(m)$); [receive (x_i, σ_i)]
2. $\forall P_i$: `BGP`((x_i, σ_i)); [$\forall P_j$ receive (($v_i^{j,0}, \sigma_i^{j,0}$), (v_i^j, σ_i^j))]
 $S_i^{v,0} := \{j \mid v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{ valid}\};$
 $S_i^v := \{j \mid v_i^j = v \wedge \sigma_i^j \text{ valid}\};$
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 $t \leq T$

validity:
 P_s 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 $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]
 $S_i^{v,0} := \{j \mid v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{ valid}\};$
 $S_i^v := \{j \mid v_i^j = v \wedge \sigma_i^j \text{ valid}\};$
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 $t \leq T$

validity:
 P_s honest

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

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 $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]
 $S_i^{v,0} := \{j \mid v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{ valid}\};$
 $S_i^v := \{j \mid v_i^j = v \wedge \sigma_i^j \text{ valid}\};$
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 $t \leq T$

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 $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]
 $S_i^{v,0} := \{j \mid v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{ valid}\};$
 $S_i^v := \{j \mid v_i^j = v \wedge \sigma_i^j \text{ valid}\};$
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 $t \leq T$

validity:
 P_s honest

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

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

1. P_s : multiseed $(m, \sigma_s(m))$; [receive (x_i, σ_i)]
2. $\forall P_i$: BGP $((x_i, \sigma_i))$; [$\forall P_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]
 $S_i^{v,0} := \{j \mid v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{ valid}\};$
 $S_i^v := \{j \mid v_i^j = v \wedge \sigma_i^j \text{ valid}\};$
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 $t \leq T$

validity:
 P_s honest

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

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

1. P_s : multiseed $(m, \sigma_s(m))$; [receive (x_i, σ_i)]
2. $\forall P_i$: BGP $((x_i, \sigma_i))$; [$\forall P_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]
 $S_i^{v,0} := \{j \mid v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{ valid}\}$;
 $S_i^v := \{j \mid v_i^j = v \wedge \sigma_i^j \text{ valid}\}$;
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 for $t > t_\sigma$
(and $x_i = m$)

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

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

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

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)

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

holds always
(for $x_i = m$)

BCEV: Validity for $t \leq T$

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

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

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

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)

elseif $|S_i^0| > |S_i^1|$ 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. $\forall P_i$: `BGP`((x_i, σ_i)); [$\forall P_j$ receive (($v_i^{j,0}, \sigma_i^{j,0}$), (v_i^j, σ_i^j))]
 $S_i^{v,0} := \{j \mid v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{ valid}\};$
 $S_i^v := \{j \mid v_i^j = v \wedge \sigma_i^j \text{ valid}\};$
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. $\forall P_i$: BGP $((x_i, \sigma_i))$; [$\forall P_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]
 $S_i^{v,0} := \{j \mid v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{ valid}\};$
 $S_i^v := \{j \mid v_i^j = v \wedge \sigma_i^j \text{ valid}\};$
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. $\forall P_i$: BGP $((x_i, \sigma_i))$; [$\forall P_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]
 $S_i^{v,0} := \{j \mid v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{ valid}\};$
 $S_i^v := \{j \mid v_i^j = v \wedge \sigma_i^j \text{ valid}\};$
 $S_i^v = S_j^v$
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)

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

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

1. P_s : multiseed $(m, \sigma_s(m))$; [receive (x_i, σ_i)]
2. $\forall P_i$: BGP $((x_i, \sigma_i))$; [$\forall P_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]
 $S_i^{v,0} := \{j \mid v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{ valid}\};$
 $S_i^v := \{j \mid v_i^j = v \wedge \sigma_i^j \text{ valid}\};$
 $S_i^v = S_j^v$
3. if $|S_i^{x_i,0}| \geq n - T \wedge |S_i^{1-x_i}| = 0$ then $y_i := x_i$ (I)
elseif $|S_i^0| > |S_i^1|$ then $y_i := 0$ else $y_i := 1$ fi. (II)

all decisions
here identical

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

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

1. P_s : multiseed $(m, \sigma_s(m));$ [receive (x_i, σ_i)]
2. $\forall P_i$: BGP $((x_i, \sigma_i));$ [$\forall P_j$ receive $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]
 $S_i^{v,0} := \{j \mid v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{ valid}\};$
 $S_i^v := \{j \mid v_i^j = v \wedge \sigma_i^j \text{ valid}\};$
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)

$S_i^v = S_j^v$

identical S_j^v

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 $((v_i^{j,0}, \sigma_i^{j,0}), (v_i^j, \sigma_i^j))$]
 $S_i^{v,0} := \{j \mid v_i^{j,0} = v \wedge \sigma_i^{j,0} \text{ valid}\};$
 $S_i^v := \{j \mid v_i^j = v \wedge \sigma_i^j \text{ valid}\};$
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)

$S_i^v = S_j^v$

identical S_j^v

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 $(b_i, \sigma_i(b_i));$ [$\forall P_j$ 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: Security for $t \leq t_\sigma$

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: Security for $t \leq t_\sigma$

1. $P_s: DS(m);$ BC for $t \leq t_\sigma$ [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: Security for $t \leq t_\sigma$

1. $P_s: DS(m);$ BC for $t \leq t_\sigma$ [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 $y_i := v;$ holds for $t \leq t_\sigma$ [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. $P_s: DS(m);$ [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. $P_s: DS(m);$ BC for $t > t_\sigma$ [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. $P_s: DS(m);$ BC for $t > t_\sigma$ [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

consistent
for $t > t_\sigma$

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

1. $P_s: DS(m);$ BC for $t > t_\sigma$ [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)]
 $M_i^v := \{\sigma_i^j \mid c_i^j = v \wedge \sigma_i^j \text{ valid}\};$ if holds then ...
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

consistent
for $t > t_\sigma$

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)]
 - $M_i^v := \{\sigma_i^j \mid c_i^j = v \wedge \sigma_i^j \text{ valid}\};$ [if holds then ...]
 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]
- 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**
also holds for same v
- fi**

HBC: Validity 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)]
 $M_i^v := \{\sigma_i^j \mid c_i^j = v \wedge \sigma_i^j \text{ valid}\};$
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: Validity for $t_\sigma < t \leq T$

1. $P_s: DS(m);$ BC for $t > t_\sigma$ [receive d_i]
2. $P_s: BCEV(m);$ guarantees validity [receive b_i]
3. Multisend $(b_i, \sigma_i(b_i));$ [$\forall P_j$ receive (c_i^j, σ_i^j)]
 $M_i^v := \{\sigma_i^j \mid c_i^j = v \wedge \sigma_i^j \text{ valid}\};$
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: Validity for $t_\sigma < t \leq T$

1. $P_s: DS(m);$ **BC for $t > t_\sigma$** [receive d_i]
2. $P_s: BCEV(m);$ **guarantees validity** [receive b_i]
3. Multisend $(b_i, \sigma_i(b_i));$ [$\forall P_j$ receive (c_i^j, σ_i^j)]
 $M_i^v := \{\sigma_i^j \mid c_i^j = v \wedge \sigma_i^j \text{ valid}\};$ **can only hold for $v = m$**
4. **if** $\exists v : |M_i^v| \geq n - t_\sigma$ **then** $DS(M_i^v)$
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: Validity for $t_\sigma < t \leq T$

1. $P_s: DS(m);$ **BC for $t > t_\sigma$** [receive d_i]
2. $P_s: BCEV(m);$ **guarantees validity** [receive b_i]
3. Multisend $(b_i, \sigma_i(b_i));$ $[\forall P_j \text{ receive } (c_i^j, \sigma_i^j)]$
 $M_i^v := \{\sigma_i^j \mid c_i^j = v \wedge \sigma_i^j \text{ valid}\};$ **can only hold for $v = m$**
4. **if** $\exists v : |M_i^v| \geq n - t_\sigma$ **then** $DS(M_i^v)$
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 **can only hold for $v = m$**
fi

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

1. $P_s: DS(m);$ BC for $t > t_\sigma$ [receive d_i]
2. $P_s: BCEV(m);$ guarantees validity [receive b_i]
3. Multisend $(b_i, \sigma_i(b_i));$ [$\forall P_j$ receive (c_i^j, σ_i^j)]
 $M_i^v := \{\sigma_i^j \mid c_i^j = v \wedge \sigma_i^j \text{ valid}\};$ can only hold for $v = m$
4. **if** $\exists v : |M_i^v| \geq n - t_\sigma$ **then** $DS(M_i^v)$
 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 d_i = m can only hold for $v = m$
fi

Conclusions

- 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

Summary of Results

- 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
$$t_c < n/2 \wedge l_r \leq l_f \leq L \wedge l_f < n/2 \wedge l_r + L < n$$
$$\wedge 2t_\sigma + L < n \wedge (t_p > 0 \Rightarrow t_p + 2L < n)$$
 - 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 $l_r \geq t_p, t_\sigma$