Privacy-enhancing auctions using rational cryptography

Peter B. Miltersen, Jesper B. Nielsen

Aarhus University

Nikos Triandopoulos

Boston University

CAGT Center for Algorithmic Game Theory

RISCS Center for Reliable Information Systems and Cyber Security

Rational cryptography

- goal: merge methodologies of cryptography & game theory

  → design & analysis of multi-agent protocols

- significant body of work

  (1) **honest, adversarial ≠ selfish & rational**

  - game-theoretic extensions of cryptographic protocols [HT04, GK06, ADGH06, LT06, KN08a, KN08b, MSR08, OPRV09, MS09, FKLN09…]

  (2) **mechanism design ≈ secure multiparty computation**

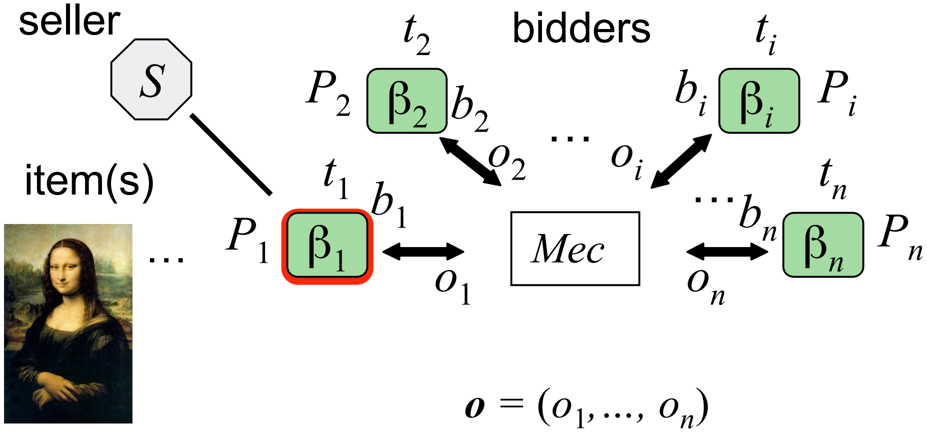
  - crypto-based realization of games without trusted mediator [DHR00, LMPS04, LMS05, ILM05,…]

- this work considers a concrete problem

  running a privacy-aware auction over the Internet

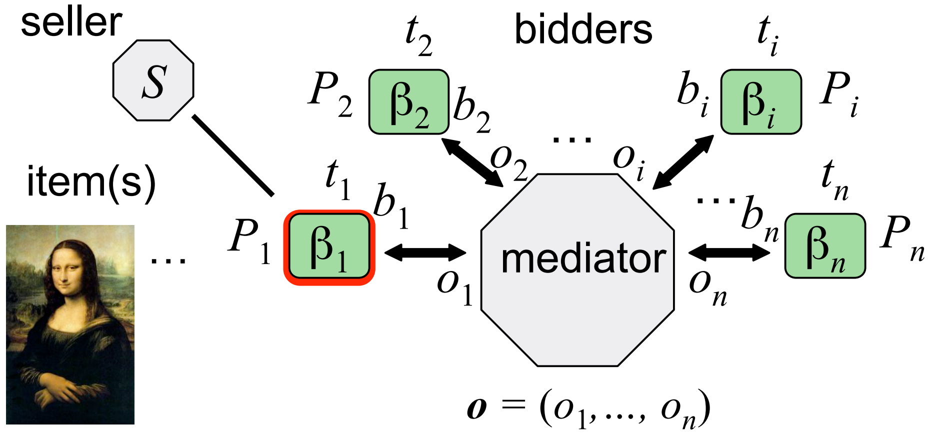
Classical auctions

- games for mapping items/prices to buyers
  (e.g., 2nd price auction)
  - distribution over private valuations or types ***t***
  - strategy β for submitting bids ***b***
  - allocation mechanism for specifying output ***o***



Classical auctions

- games for mapping items/prices to buyers
  (e.g., 2^{nd} price auction)
  - distribution over private valuations or types $\boldsymbol{t}$
  - strategy β for submitting bids $\boldsymbol{b}$
  - allocation mechanism for specifying output $\boldsymbol{o}$



mediated

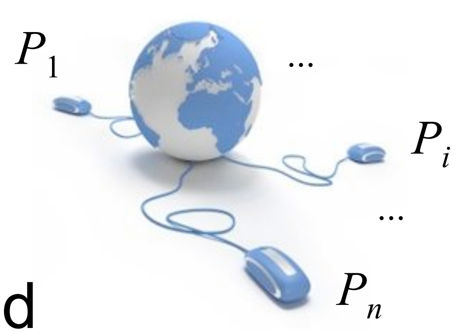
- defined by an abstract functionality
- realized through a concrete implementation

privacy-oblivious

- monetary utilities
- private bids/types may be revealed to participants

The problem

- goal: design an auction protocol for the Internet which considers privacy and which is rational to follow
- we wish the auction game to be



+

rich prior work, e.g., [NPS99, PRST06…]

Internet-based

- use realistic communication
  - secure & authenticated **point-to-point channels**
- towards practical implementation

privacy-aware

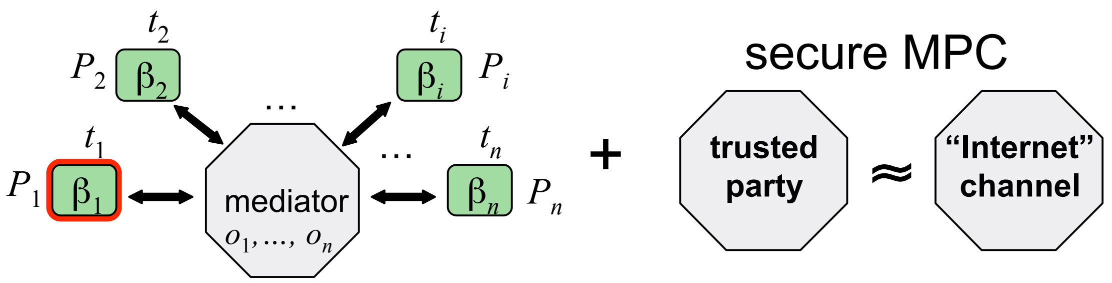
- model privacy concerns
  - bidders wish to prevent revealing information related to their valuations but would appreciate learning others’ valuations
- protect bidders’ valuations

Challenges

- goal: design an **auction** protocol for the **Internet** which considers **privacy** and which is **rational** to follow

Challenges

- goal: design an **auction** protocol for the **Internet** which considers **privacy** and which is **rational** to follow



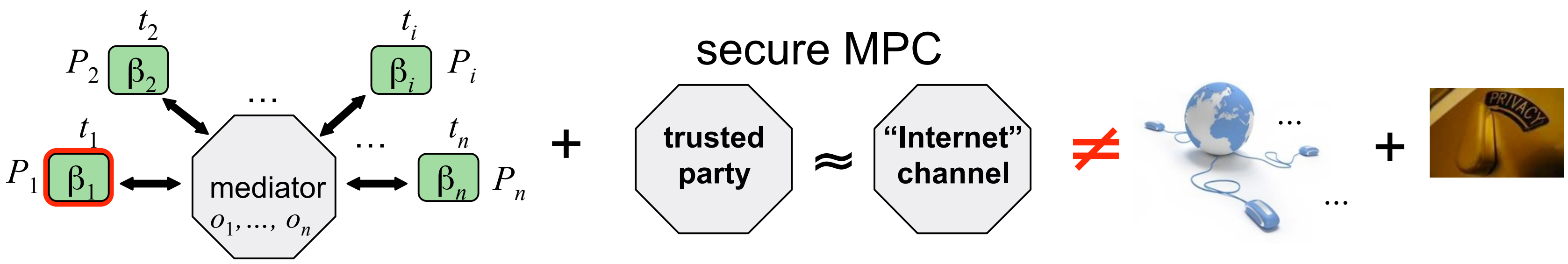
"use secure MPC to implement your favorite auction"

such an approach is insufficient

- **rational execution**
  - equilibrium analysis for secure privacy-aware auction in computational setting
- **information leakage**
  - consistent model for any information leakage that occurs in mediated auction
- **transaction completion**
  - definition of "winning" state given that winner is never forced to buy

Challenges

- goal: design an **auction** protocol for the **Internet** which considers **privacy** and which is **rational** to follow



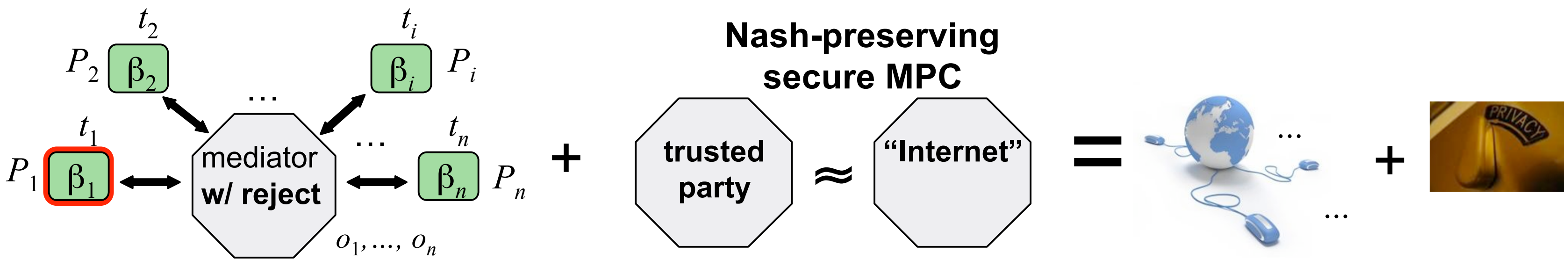
at least, not yet…

such an approach is insufficient

- **rational execution**
  - equilibrium analysis for secure privacy-aware auction in computational setting
- **information leakage**
  - consistent model for any information leakage that occurs in mediated auction
- **transaction completion**
  - definition of “winning” state given that winner is never forced to buy

Our approach

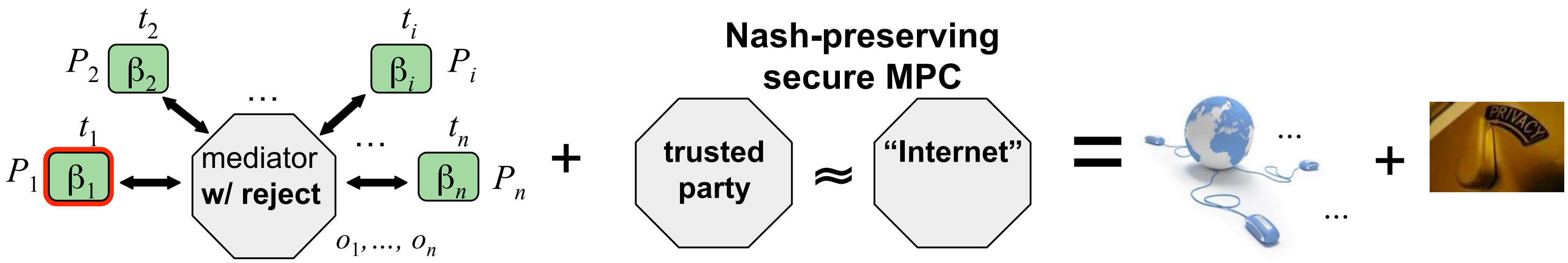
- rectify previous unsuccessful attempt



- define appropriate game-theoretic framework
  - protocol games over the Internet w/ hybrid utility model → **rational execution**
  - privacy-enhanced approximate Nash (PE ε-Nash) → **information leakage**
  - contracts and mediation w/ reject → **transaction completion**
- design Internet-based Nash-preserving sec-MPC protocol
  - unknown contract revelation point → **participation**
  - decoupling of winning information and winning contracts → **multi-winners**

Our result

- general design principle and possibility result



consider any PE ε-Nash auction mech. in the mediated w/ reject setting

generic method for Internet-based Nash implementation

PE ε-Nash auction mech. in the Internet setting with utility profile **negligibly close** to the original one

do such mechanisms exist?
yes, all "**predictable**" ones
(e.g., 1^{st} price auctions)

condition: players' "expected fiscal utility" sufficiently larger than "privacy weight", i.e., "greedy-then-paranoid"

≠

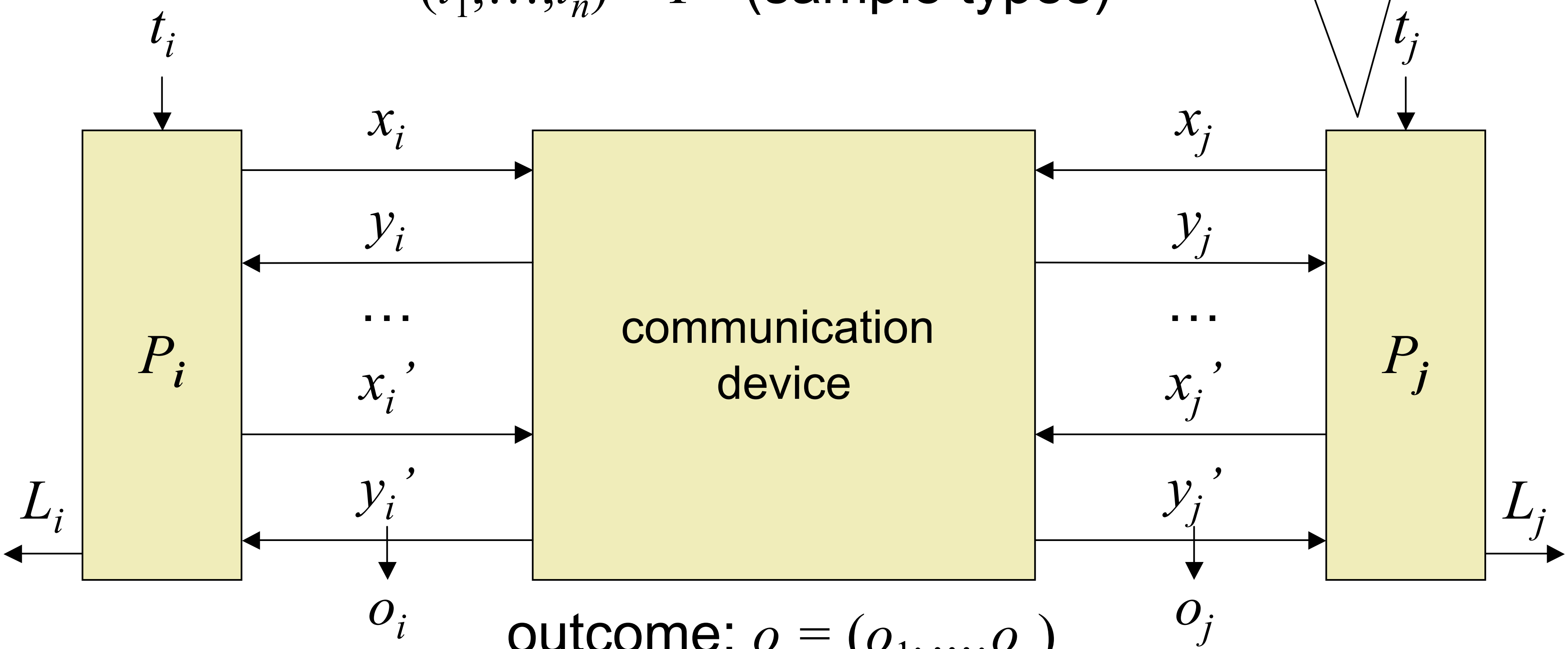
2^{nd} price auctions

formal framework for "composable" Nash-preserving transformations from abstract to concrete settings

Protocol games

strategy $\sigma(k) \in A^{T(k)}$: non-uniform family of circuits, one for each security parameter k

$(t_1,\ldots,t_n) \leftarrow T$ (sample types)

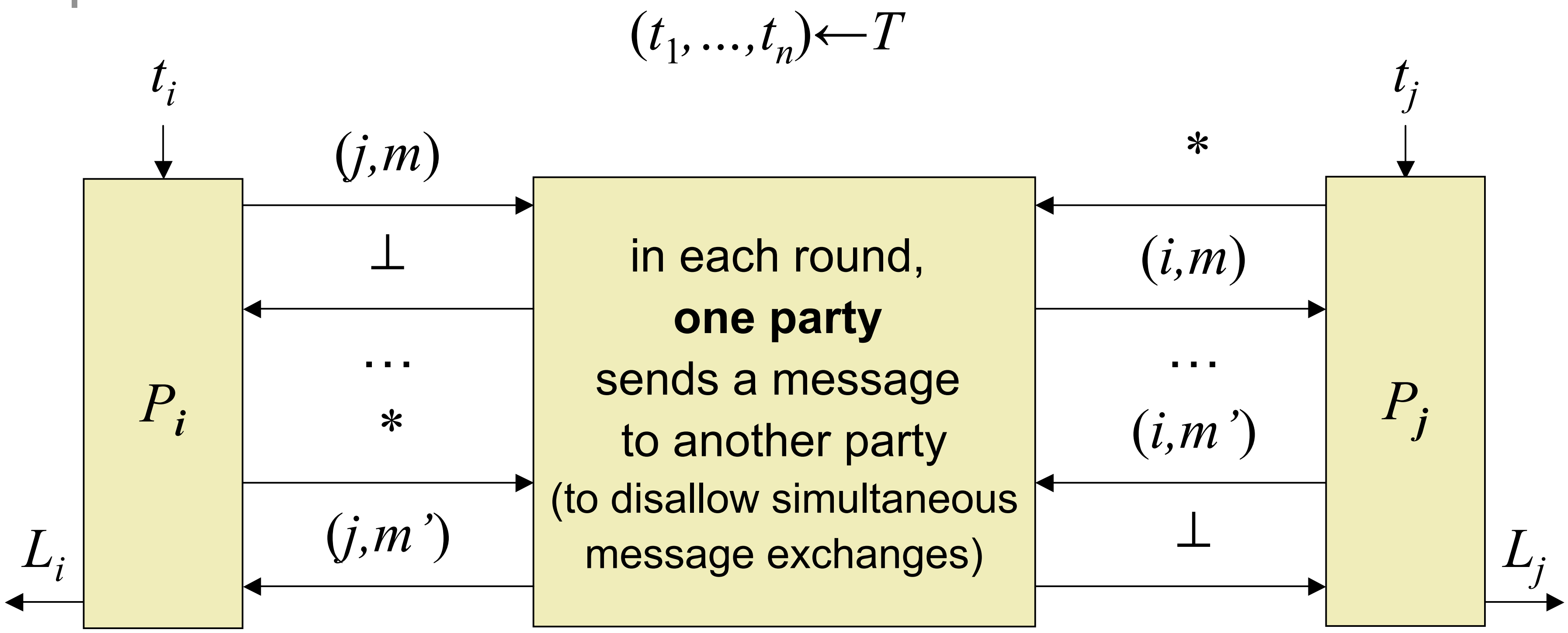


outcome: $o = (o_1, \ldots, o_n)$

local output: $L=(L_1, \ldots, L_n)$

“normal” utility: $u_i(t,o)$, privacy-aware utility: $u_i(t,o,L)$

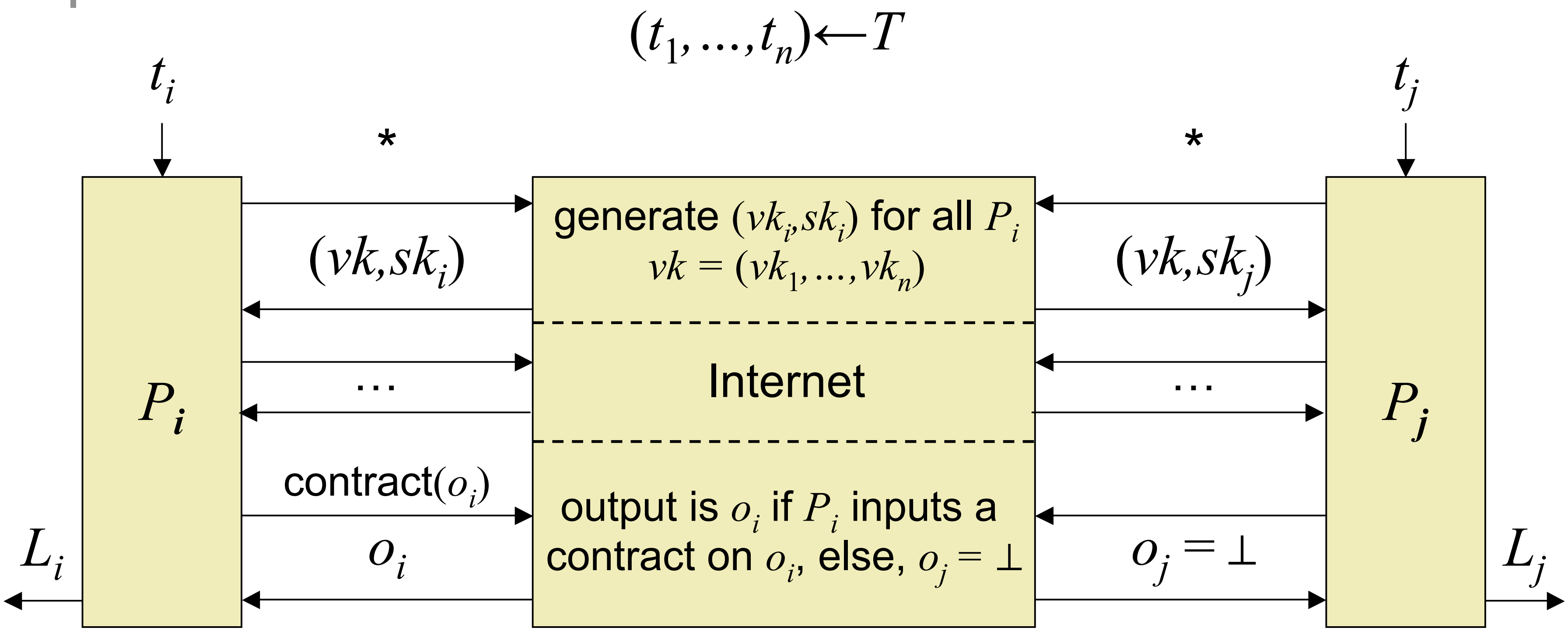
Internet-like communication



what about the protocol outputs?

- defined by **contracts**
  - “winning-state” values that are signed by all parties (using a PKI)

PKI + Internet + Contracts


$(t_1, \ldots, t_n) \leftarrow T$
t_i
t_j
*
*
P_i
P_j
generate (vk_i, sk_i) for all P_i
$vk = (vk_1, \ldots, vk_n)$
(vk, sk_i)
(vk, sk_j)
Internet
…
…
contract(o_i)
o_i
output is o_i if P_i inputs a contract on o_i, else, $o_j = \perp$
$o_j = \perp$
L_i
L_j

we assume that fiscal utility is 0 if $o_j = \perp$

Hybrid utility model

- utility of P_i is a sum of a **fiscal** utility f_i and a **privacy** utility p_i

$$u_i(t,o,L) = f_i(t,o) + p_i(t,L)$$

- we model fiscal preferences using a utility function $f_i(t,o) \in \boldsymbol{R}$
  - its output is polynomial in k
- we model privacy concerns using a utility function $p_i(t,L) \in \boldsymbol{R}$
  - poly-time computable in k
  - it does not significantly value loss of own information
    - e.g., $p_1(t,(\perp,L_2,\ldots,L_n)) - p_1(t,(L_1,L_2,\ldots,L_n)) \leq negl(k)$

we call such a privacy utility **admissible**

different hybrid model [HP08]

Greedy-then-paranoid

- we assume that parties are **greedy-then-paranoid**
  - first and foremost they want the good, but all other things being equal they also value privacy
  - in particular: not willing to always bid b_i=0 just to hide information on their type
- we define **privacy weight**

$$\begin{aligned} p &= (p_1, \ldots, p_n) \\ pw(p_i) &= max_X\, p_i(X) - min_X\, p_i(X) \\ pw(p) &= max_i\, pw(p_i) \end{aligned}$$

BIG BUSINESS
WAR
PROFITS FROM BUILDING MATERIAL
PROFITS FROM PEOPLE'S FOOD
WAR PRICES
PROFITS FROM WAR-PRICED CLOTHING
INTEREST ON WAR LOANS
PROFITS FROM WAR SUPPLIES

Privacy-enhanced ε-Nash

- **deviation incentive** of protocol $\sigma = (\sigma_1, \ldots, \sigma_n)$

  $\varepsilon(k) \;= max\ P_i,\ max\ \sigma_i{}^*(k) \in A^{T(k)}$: $u_i(\ \sigma_i{}^*(k), \sigma_{-i}(k)\ ) - u_i(\sigma)$

- σ is ε-Nash if its deviation incentive is negligible in k for all $T(k)$

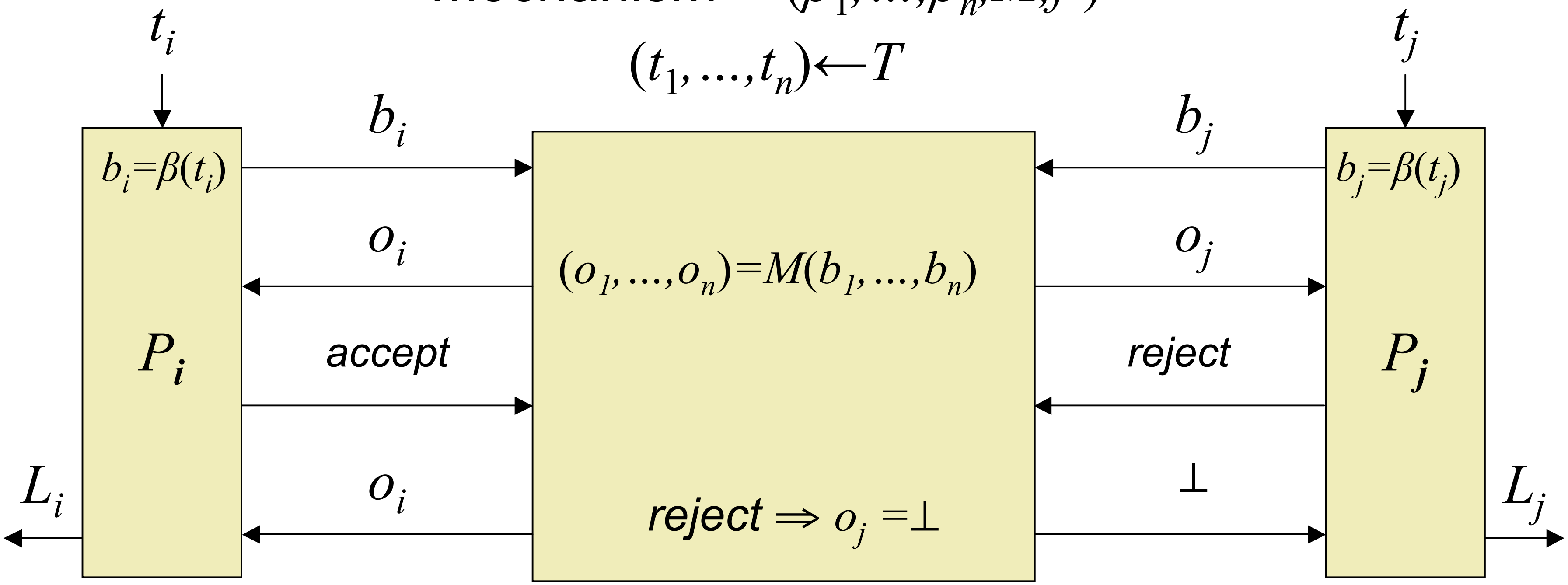
- a mechanism is a **privacy-enhanced** ε-Nash, for privacy weight α and fiscal utilities f, if it is an ε-Nash for

  $$u_i(t,o,L) = f_i(t,o) + p_i(t,L)$$

  for **all** admissible p, $pw(p) \leq \alpha,$ and polynomial strategy spaces A^T

Mediated setting w/ reject

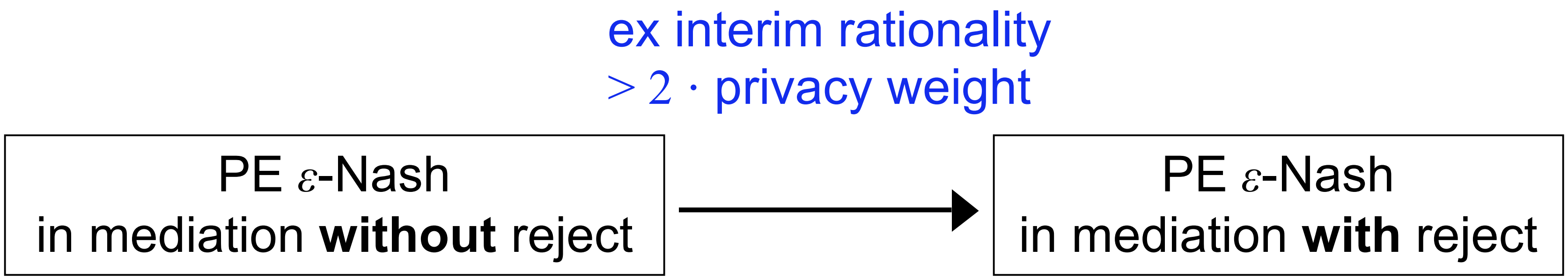
mechanism = $(\beta_1, \ldots, \beta_n, M, f)$



only interested in recommended protocols which play *accept*

Auctions in mediation w/ reject

- 2^{nd} price auctions **are not** PE ε-Nash, $\alpha > 0$
  - rational to bid the maximal price and throw away the contract if you do not like the price
- 1^{st} price auctions **are** PE ε-Nash, suff. small α
  - e.g., a mechanism with strict *ex interim* rationality: after seeing your type your expected utility is never 0



ex interim rationality
$> 2 \cdot$ privacy weight

PE ε-Nash
in mediation **without** reject

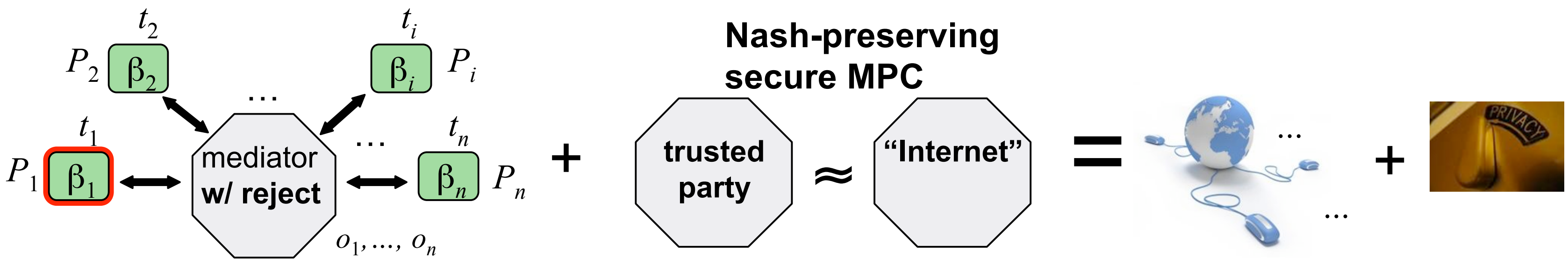
PE ε-Nash
in mediation **with** reject

ex interim rationality
minimum over all P_i
expected utility after seeing t_i

true for any **predictable** mechanism:
expected fiscal utility of a winner P_i
depends only on b_i

Our approach

- general design principle and possibility result



- define appropriate game-theoretic framework
  - protocol games over the Internet w/ hybrid utility model √
  - privacy-enhanced approximate Nash (PE ε-Nash) √
  - contracts and mediation w/ reject √
- design Internet-based Nash-preserving sec-MPC protocol
  - generic Nash-preserving transformation of any mechanism with strict ex interim rationality achieving utility profiles negligibly close to original protocol

Basic idea, a problem and a fix

<u>idea</u> - one winner case

- use sec-MPC to compute an **additive secret sharing** of the contract
- make the shares of the contract public in round robin order
  - if any party withholds share, penalize by also withholding

<u>intuition</u>

- until the last share is made public nobody knows the contract and therefore no party can exclude that it won
- sending ones’ output share is rational by strict *ex interim* rationality

Basic idea, a problem and a fix

<u>idea</u> - one winner case

- use sec-MPC to compute an **additive secret sharing** of the contract
- make the shares of the contract public in round robin order
  - if any party withholds share, penalize by also withholding

<u>intuition</u>

- until the last share is made public nobody knows the contract and therefore no party can exclude that it won
- sending ones' output share is rational by strict *ex interim* rationality

<u>problem</u>

- the last party will know who won and might not make its share public when it is not the winner

<u>fix</u>

- let the winner hold the last share!

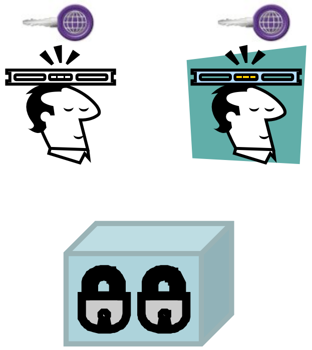
…and another problem

- if by definition the winner is last in the round-robin, then all the n-1 first parties know they did not win
  - makes it rational for them to stay silent!

monetary value for the winner,
but privacy value for other parties

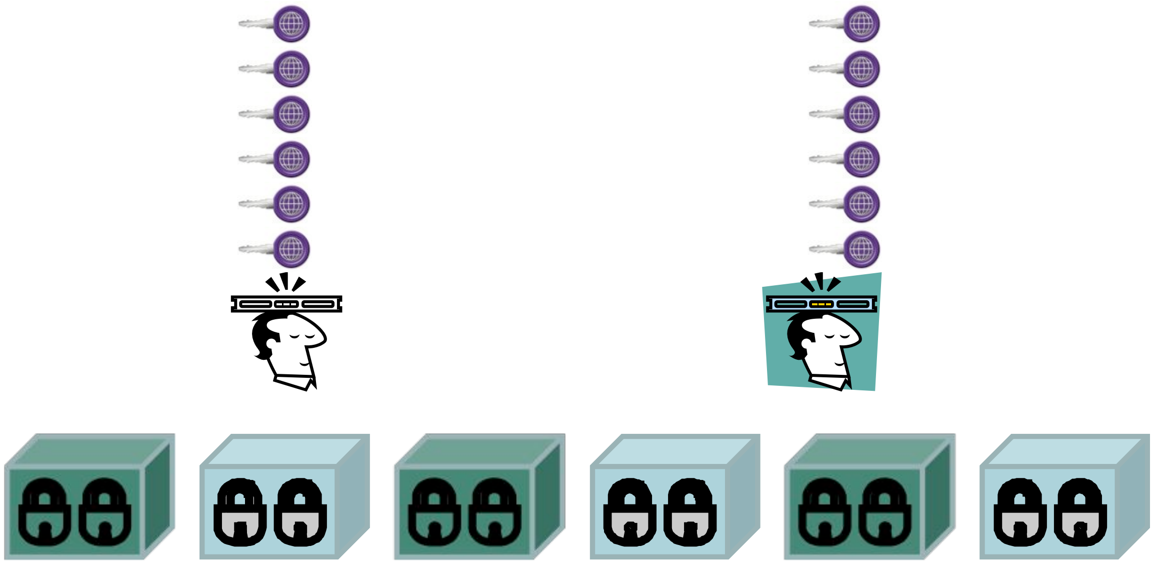
contract

who sends a key first?



Fix: multi-phase protocol

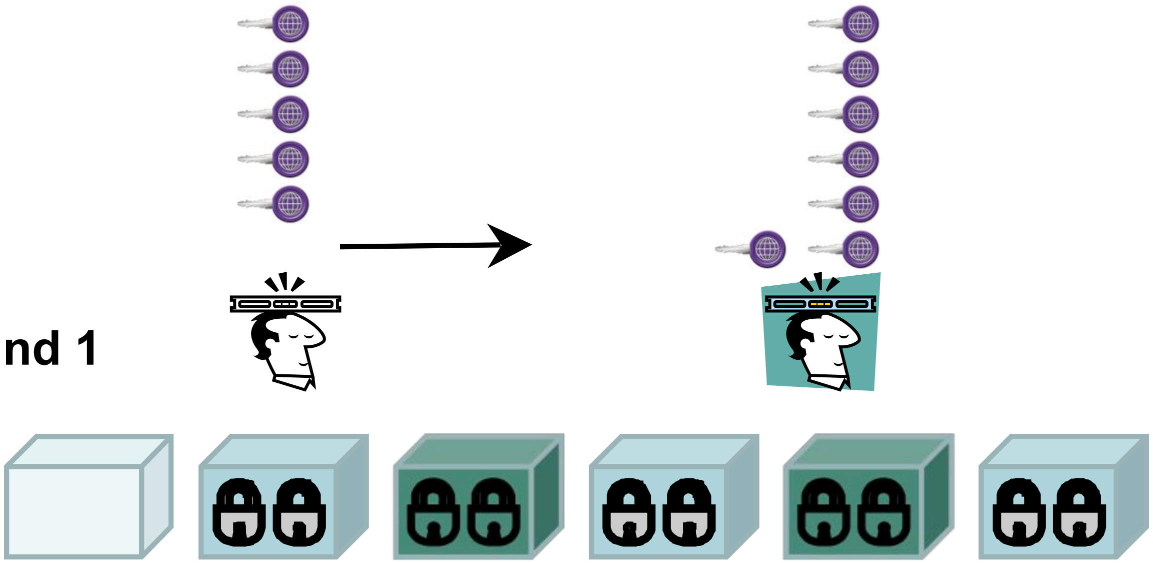
- create many ($O(k)$) boxes (standard trick [HT04,GK06,LT06,GHKL08,KN08])
  - all boxes are empty holding $\perp$, expect the π-th box holding the contract
  - pick π s.t. $Pr[\pi = p] = \tfrac{1}{2}^{p}$; keep π unknown
  - the i-th box stores the output of party $P_{i \bmod n}$
  - unlock i-th box in n rounds, by revealing shares to $P_{i \bmod n}$ in round robin
  - if a party does not reconstruct $\perp$ or a valid contract it stays silent for ever



Fix: multi-phase protocol

- create many ($O(k)$) boxes (standard trick [HT04,GK06,LT06,GHKL08,KN08])
  - all boxes are empty holding ⊥, expect the π-th box holding the contract
  - pick π s.t. $Pr[\pi = p]=½^p$; keep π unknown
  - the i-th box stores the output of party $P_{i \bmod n}$
  - unlock i-th box in n rounds, by revealing shares to $P_{i \bmod n}$ in round robin
  - if a party does not reconstruct ⊥ or a valid contract it stays silent for ever

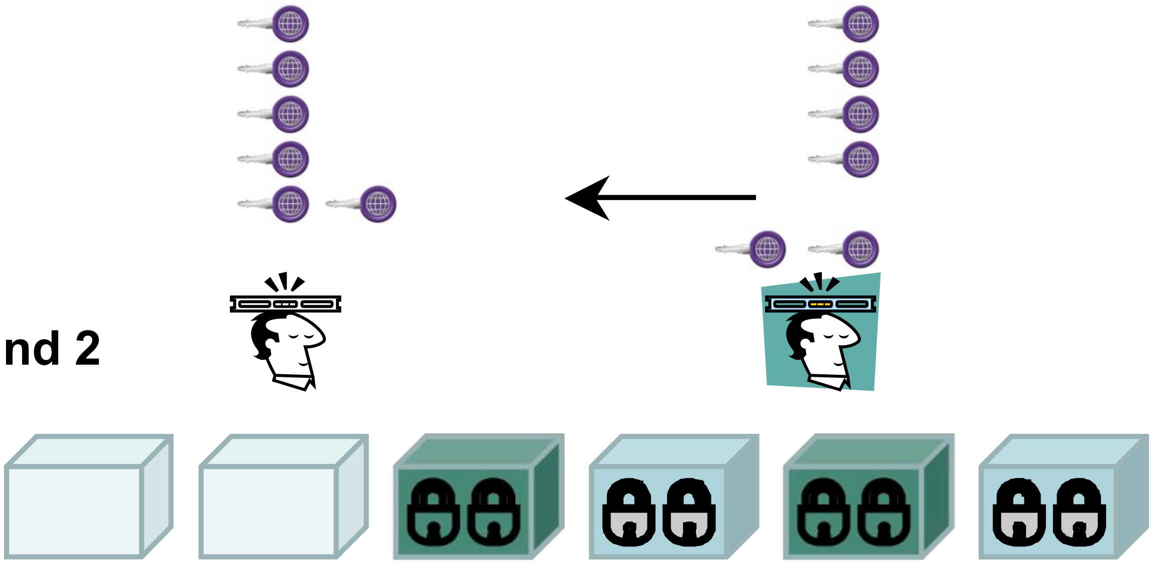
phase 1, round 1



Fix: multi-phase protocol

- create many $(O(k))$ boxes (standard trick [HT04,GK06,LT06,GHKL08,KN08])
  - all boxes are empty holding $\perp$, expect the π-th box holding the contract
  - pick π s.t. $Pr[\pi = p]=\frac{1}{2}^{p}$; keep π unknown
  - the i-th box stores the output of party $P_{i \bmod n}$
  - unlock i-th box in n rounds, by revealing shares to $P_{i \bmod n}$ in round robin
  - if a party does not reconstruct $\perp$ or a valid contract it stays silent for ever

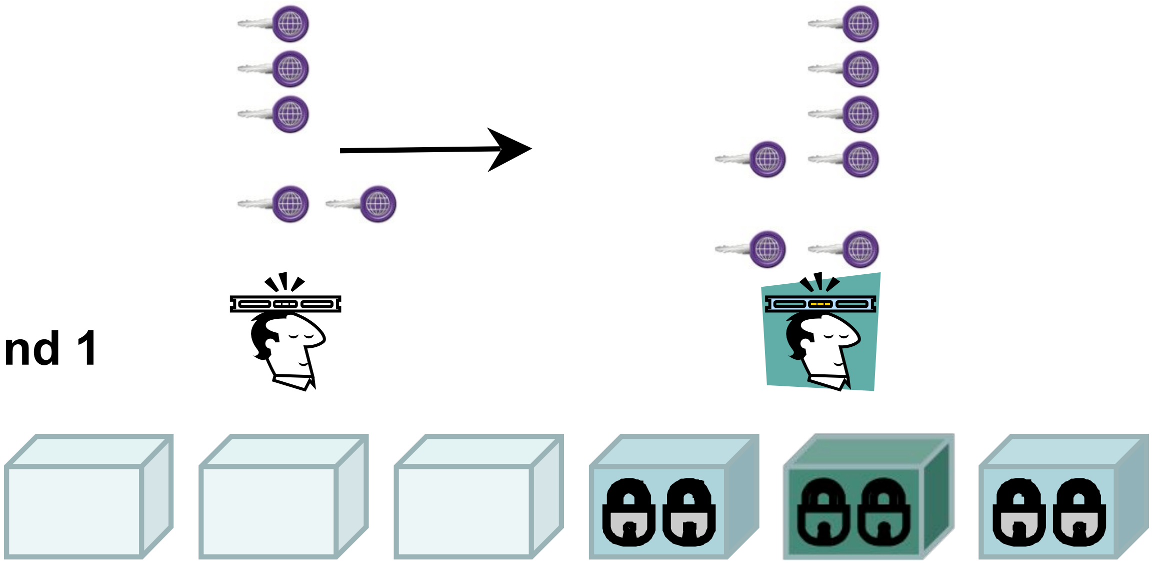
phase 1, round 2



Fix: multi-phase protocol

- create many ($O(k)$) boxes (standard trick [HT04,GK06,LT06,GHKL08,KN08])
  - all boxes are empty holding ⊥, expect the π-th box holding the contract
  - pick π s.t. $Pr[\pi = p] = ½^p$; keep π unknown
  - the i-th box stores the output of party $P_{i \bmod n}$
  - unlock i-th box in n rounds, by revealing shares to $P_{i \bmod n}$ in round robin
  - if a party does not reconstruct ⊥ or a valid contract it stays silent for ever

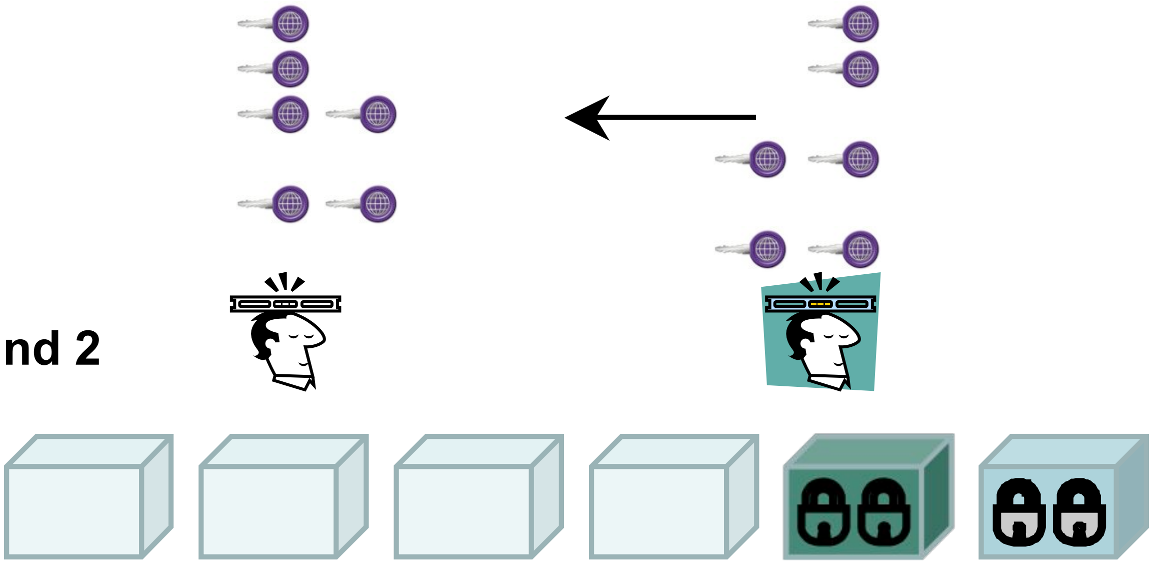
phase 2, round 1



Fix: multi-phase protocol

- create many ($O(k)$) boxes (standard trick [HT04,GK06,LT06,GHKL08,KN08])
  - all boxes are empty holding ⊥, expect the π-th box holding the contract
  - pick π s.t. $Pr[\pi = p] = {}^{1}\!/_{2}{}^{p}$; keep π unknown
  - the i-th box stores the output of party $P_{i \bmod n}$
  - unlock i-th box in n rounds, by revealing shares to $P_{i \bmod n}$ in round robin
  - if a party does not reconstruct ⊥ or a valid contract it stays silent for ever

phase 2, round 2

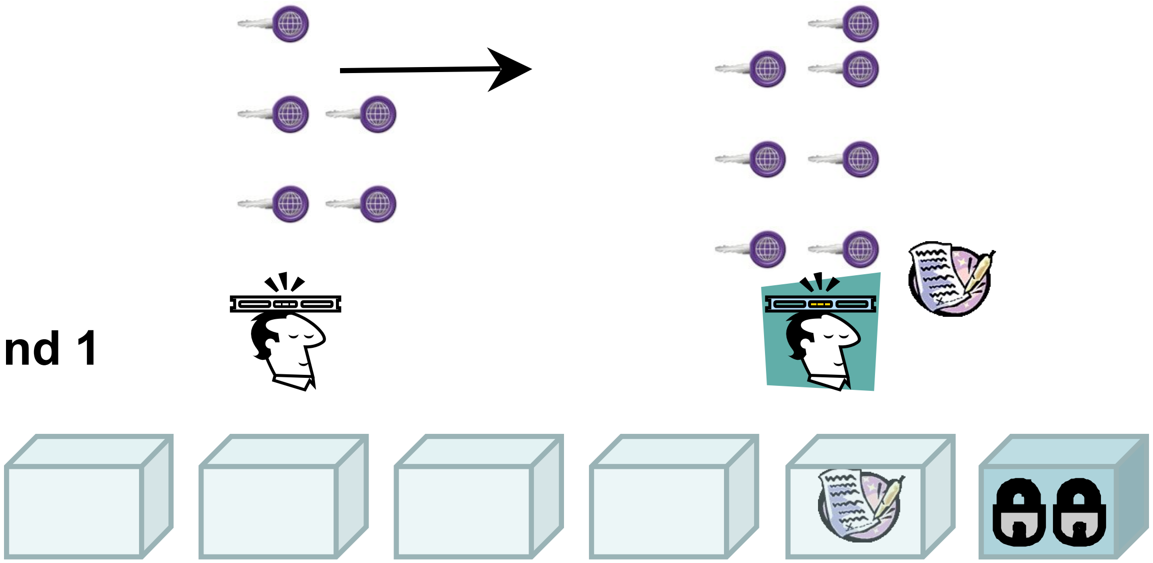


Fix: multi-phase protocol

- create many ($(O(k))$) boxes (standard trick [HT04,GK06,LT06,GHKL08,KN08])
  - all boxes are empty holding $\perp$, expect the π-th box holding the contract
  - pick π s.t. $Pr[\pi = p]=½^p$; keep π unknown
  - the i-th box stores the output of party $P_{i \bmod n}$
  - unlock i-th box in n rounds, by revealing shares to $P_{i \bmod n}$ in round robin
  - if a party does not reconstruct $\perp$ or a valid contract it stays silent for ever

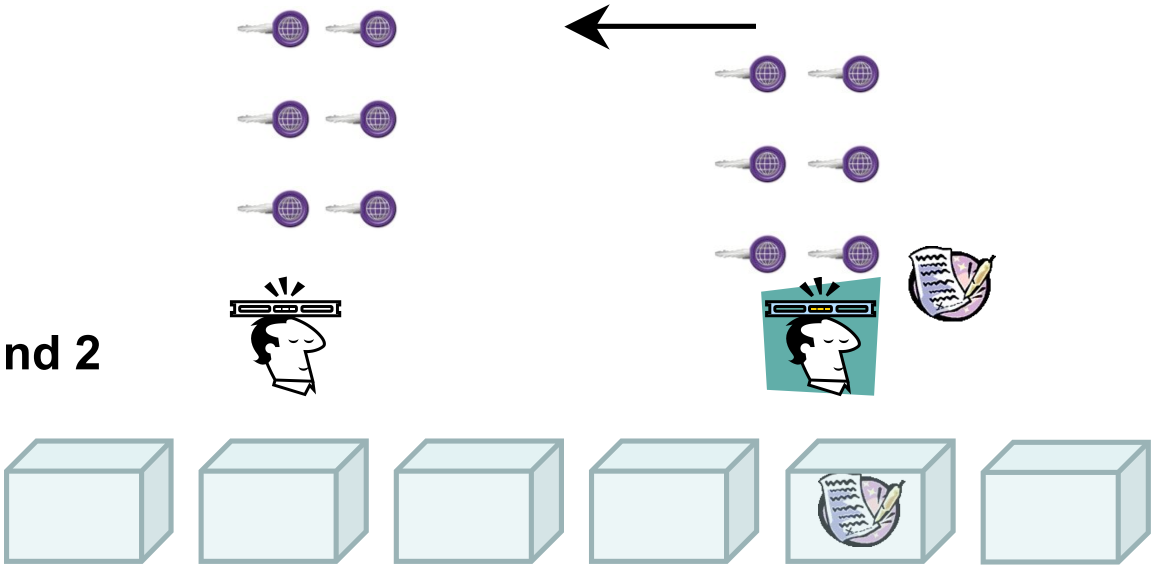
right party
gets contract

phase 3, round 1



Fix: multi-phase protocol

- create many ($O(k)$) boxes (standard trick [HT04,GK06,LT06,GHKL08,KN08])
  - all boxes are empty holding $\perp$, expect the π-th box holding the contract
  - pick π s.t. $Pr[\pi = p]=½^p$; keep π unknown
  - the i-th box stores the output of party $P_{i \bmod n}$
  - unlock i-th box in n rounds, by revealing shares to $P_{i \bmod n}$ in round robin
  - if a party does not reconstruct $\perp$ or a valid contract it stays silent for ever



protocol completed

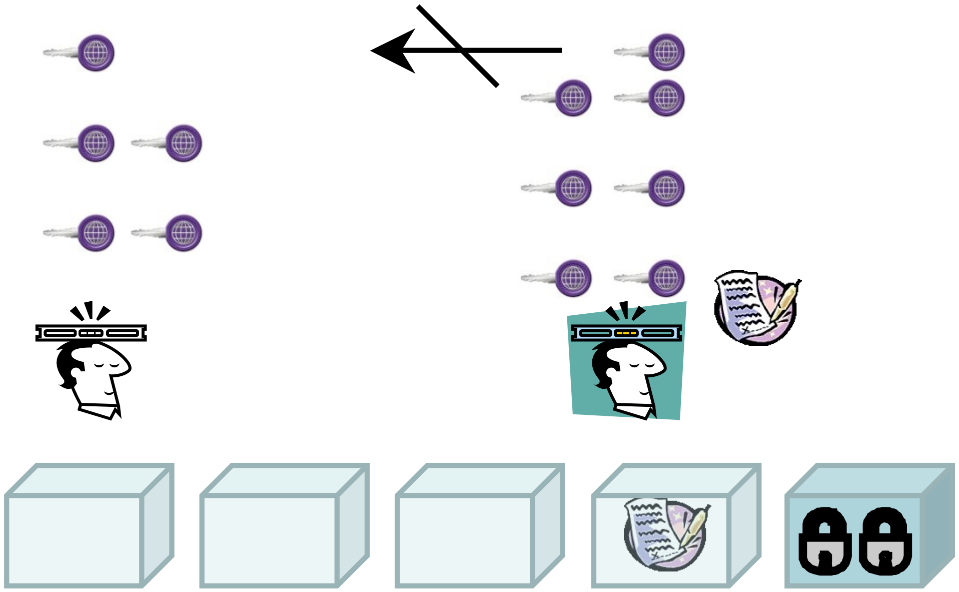
phase 3, round 2

More winners – first attempt

- if there are more winners, all contracts are handed out right after each other (in the same phase)
- what will really happen?
  - the first (e.g., right) winner prevents the information in the second (e.g., left party's) contract from leaking by withholding its shares

right party **does not** send its share to left party

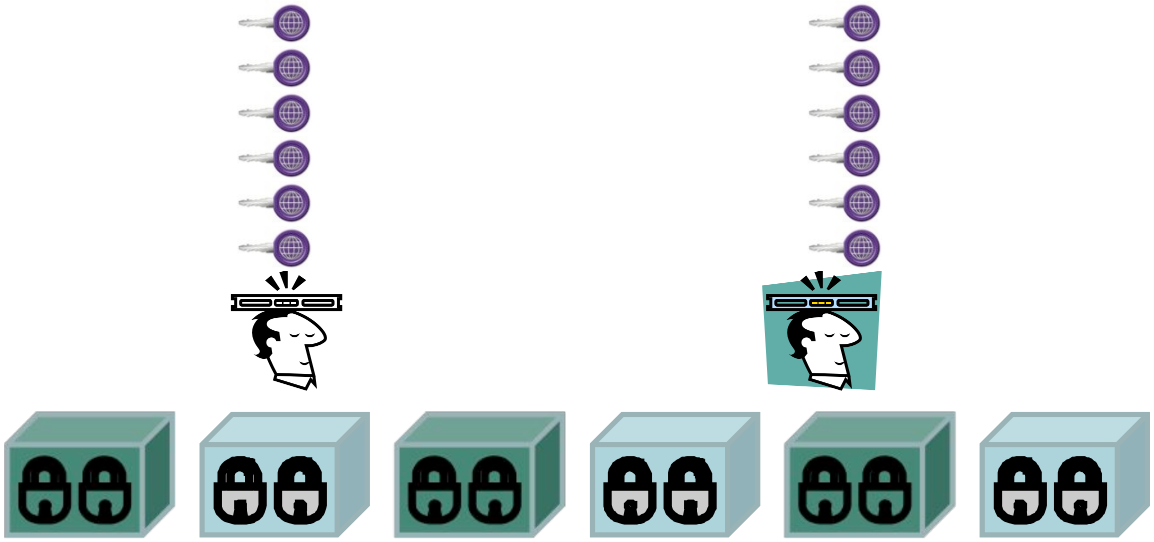
phase 3, **round 3**



More winners – fix

decouple the *information* and the *contract*

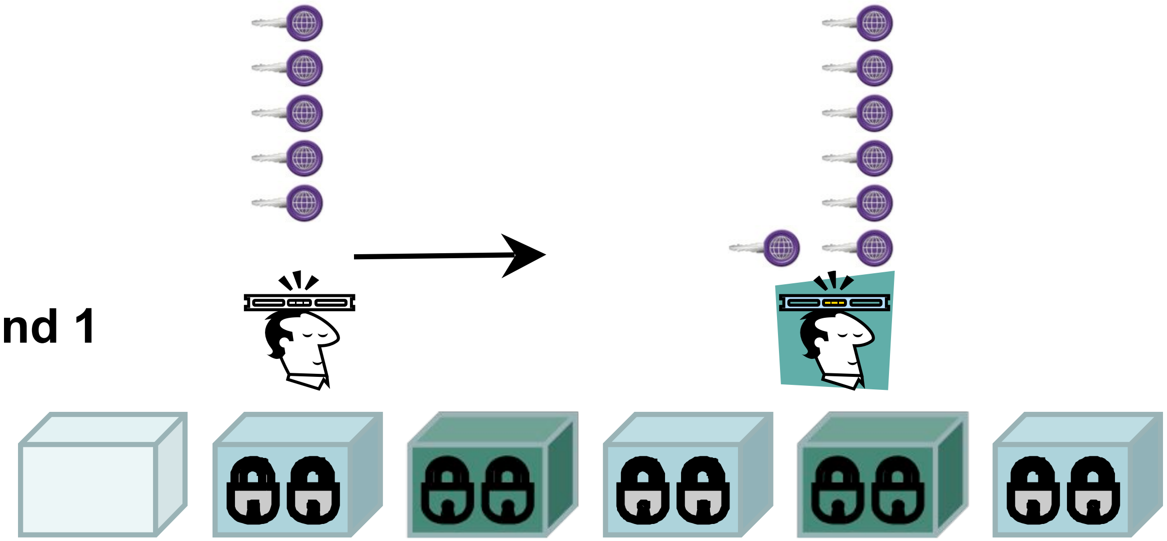
- first leak the **information** of the contracts, “P_i won item G at price is p”
- then provide the contracts, the signature on this info, in the **next phase**



More winners – fix

decouple the *information* and the *contract*

- first leak the **information** of the contracts, “P_i won item G at price is p”
- then provide the contracts, the signature on this info, in the **next phase**

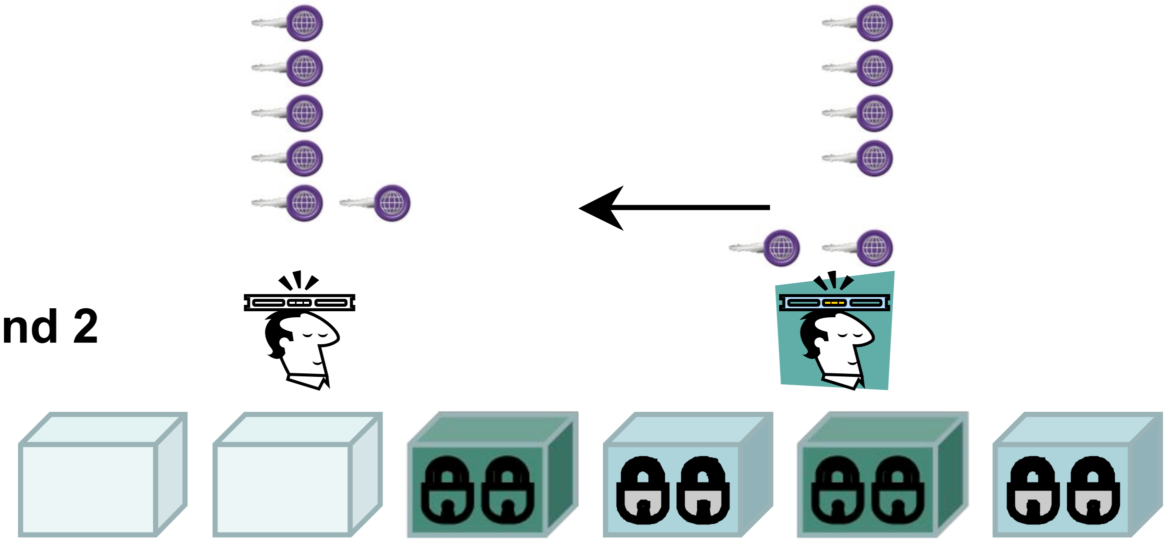


phase 1, round 1

More winners – fix

decouple the *information* and the *contract*

- first leak the **information** of the contracts, “P_i won item G at price is p”
- then provide the contracts, the signature on this info, in the next phase



phase 1, round 2

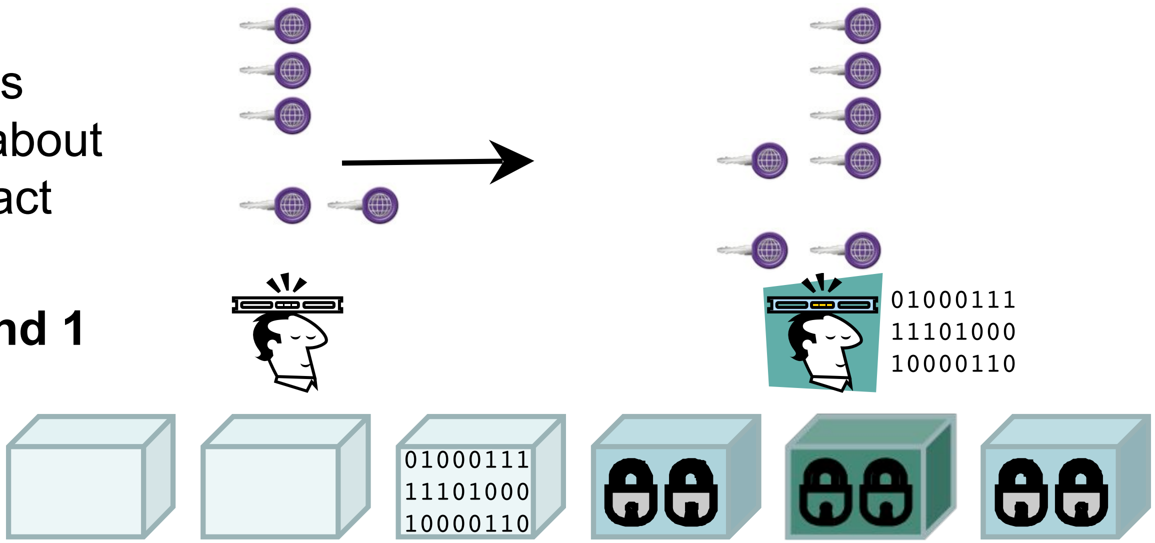
More winners – fix

decouple the *information* and the *contract*

- first leak the **information** of the contracts, “P_i won item G at price is p”
- then provide the contracts, the signature on this info, in the **next phase**

right party gets **information** about winning contract

phase 2, **round 1**



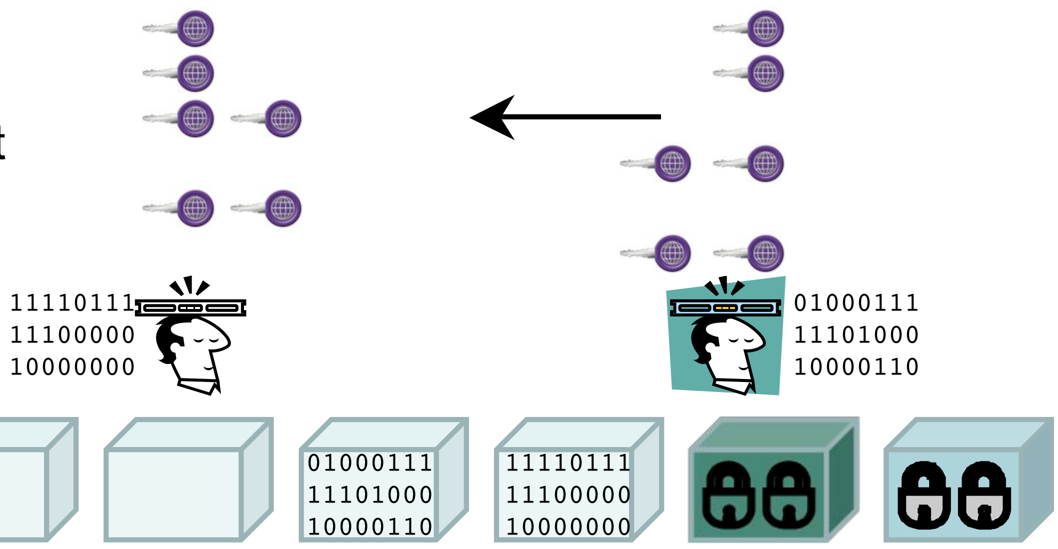
More winners – fix

decouple the *information* and the *contract*

- first leak the **information** of the contracts, “P_i won item G at price is p”
- then provide the contracts, the signature on this info, in the **next phase**

left party gets **information** about winning contract

phase 2, **round 2**



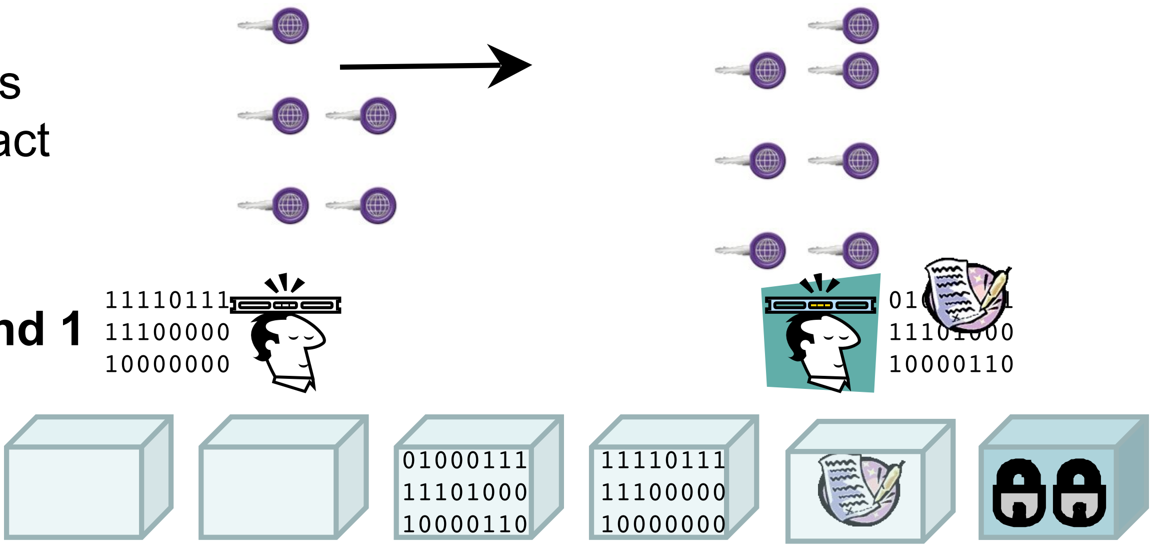
More winners – fix

decouple the *information* and the *contract*

- first leak the **information** of the contracts, “P_i won item G at price is p”
- then provide the contracts, the signature on this info, in the **next phase**

right party gets
winning contract

phase 3, round 1



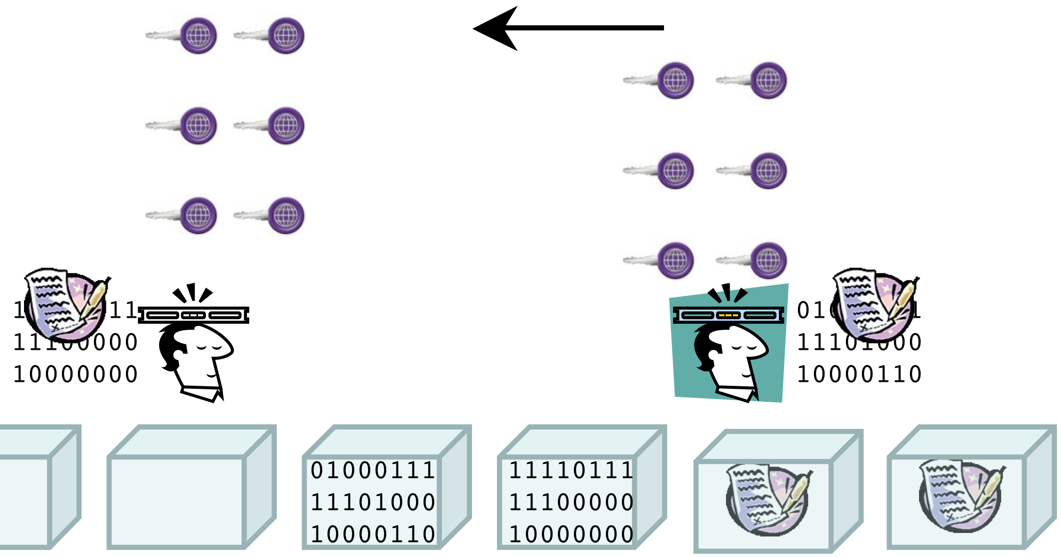
More winners – fix

decouple the *information* and the *contract*

- first leak the **information** of the contracts, “P_i won item G at price is p”
- then provide the contracts, the signature on this info, in the **next phase**

left party gets
winning contract

phase 3, **round 2**



Conclusions

- privacy-enhancing auctions
  - first example on practical rational MPC in Internet-like settings
  - inherent limitations (1st Vs. 2nd price auction separation)
  - generic framework for Nash-implementation
- future directions
  - too young area; we are far from having a good understanding
  - towards privacy-aware computational/distributed mechanism design

Thank you