# Fair Computation with Rational Players

## Sufficient conditions for getting rationally fair MPC protocol with Computational Nash Equilibrium


Authors:

Amos Beimel  Adam Groce

Jonathan Katz  Ilan Orlov

Presented by:

Shubh Prakash


November 6, 2023

# Outline

# Outline

# Why connect Game Theory and Cryptography?

- Game Theory and cryptography both involve interactions between mutually distrusting parties
- Each party has its own interests
- But the parties need to interact to compute some function for example
- Usually in the interaction, the parties are supposed to follow a protocol
- It is important to protect the honest parties if some corrupt party decides to deviate from the protocol
- Cryptography considers **arbitrary deviations** from the protocol(malicious parties)
- Game Theory treats the protocol as a game and the parties as players in the game who have some utilities and they want to maximise it(rational players)
- So, game theory considers **only rational deviations**
- So, it is very natural to look at game theory and cryptography together and see how techniques from one field can apply to the other

# Game Theory in cryptography

- Suppose there is a cryptographic multiparty protocol in which the parties can deviate arbitrarily
- Because deviations can be arbitrary, it may not be possible to achieve feasibility results in many natural cases
- Game Theory can be used to **potentially circumvent some of the impossibility results in cryptography**
- This is done by considering rational parties instead of malicious parties

# Cryptography in Game Theory

- There can be games involving a trusted mediator(who is not a player in the game)
- It might be desirable to remove the dependency on the trusted mediator
- For this, the **trusted mediator can potentially be replaced with a cryptographic protocol** which is run by the players of the game themselves
- So this is how cryptography can be used in game theory

# Focus of this work

This work can be looked at from both aspects

1. Game theory in cryptography:
   - The notion of fairness in a protocol doing some computation is defined
   - Fairness means that all honest parties in the protocol should get the correct output of the computation which the protocol is doing
   - That is, if the computation is of a function $f$, then all honest parties should learn the value of $f$ on the true inputs of all the parties
   - There are some cryptographic impossibility results known for fairness in the case where parties are malicious
   - This work considers parties to be rational and tries to circumvent the impossibility results in some cases
2. Cryptography in game theory
   - The problem of fair computation can be looked at as a game with all (rational in this case) parties giving their inputs to the trusted mediator who computes the function and gives the output to all the parties(ideal world)
   - This work tries to find sufficient conditions for when the trusted mediator can be got rid of from the game and can be replaced by a cryptographic protocol executed by the parties themselves

# Outline

# Fairness in malicious setting

- There are impossibility results which show that fairness is impossible to achieve if a majority of the parties are malicious
- This is mainly because malicious means arbitrary deviations are possible by the corrupt parties
- Thus, it is extremely hard to come up with protocols that will protect the honest minority from the corrupt majority
- So, **there is need to make the adversary weaker and circumvent the impossibility**

# Fairness in rational setting

- There is a negative result by Asharov et al. in this regard
- A particular $f$, a particular input distribution, and a specific utility function is considered
- Then, it is shown that there cannot be any rationally fair protocol(with correctness greater than 0.5) which can compute $f$ under the given utilities and input distributions(under fail-stop deviations)
- This negative result is in a very special case
- There is a **need to try to see what "sufficient conditions" this specific case doesn't satisfy and try to give positive results when the sufficient conditions is satisfied**

# Contributions of this work

- This work shows a broad feasibility result that if the adversary is weakened to be only rational, **then the impossibility of fair computation with honest minority can be circumvented**
- It also gives a sufficient condition for when rationally fair protocols are possible in the real world(the sufficient conditions are to be satisfied in the ideal world)
- The function $f$ can be arbitrary, so can the input distributions and the utility functions
- The deviations considered are both fail stop and byzantine
- Another interpretation is that if the game with a trusted mediator satisfies some sufficient conditions regarding its equilibrium, then the **trusted mediator can be replaced with a protocol run by the players themselves and that "preserves the equilibrium" of the original game**

# Outline

# Negative result regarding fairness in rational setting

- The negative result given by Asharov et al. is in a setting where the **rational parties have no incentive to compute the function by following any protocol**(even in ideal world where fairness is guaranteed)
- Its a 2 player setting, the function is bit XOR, inputs $x_1, x_2$ are uniform and independent
  Utilities:
- Utility function is same for $P_1, P_2$
- Utility for $P_1$ is 1 if it gets correct output and $P_2$ gets wrong output
- It is -1 if it gets wrong output and $P_2$ gets correct
- It is 0 in all other cases
- The **expected utility for a player is the same** whether it participates in any protocol which correctly and fairly computes $f$ or whether it just guesses the other parties input and computes $f$ by itself
- So, an ideal world computation of this $f$(under this setting) is **not a strict Nash Equilibrium**

# Rational Secret Sharing

- There is a lot of work on rational secret sharing
- The results of this work can be considered as a generalization of rational secret sharing
- As rational secret sharing deals with a specific function, a specific choice of utilities and instead of an input distribution, there is a dealer who generates the inputs
- As a result **this work can be used to get rational secret sharing schemes as a special case**(though the equilibrium achieved is weaker)

# Other related work

- There are some other results which try to do similar things
- But the assumptions are either too strong, or what they obtain is weaker than this work
- Another possibility is that those results are not as general as this work

# Outline

# Rationally Fair Protocol

- This work defines the notion of when a protocol is *rationally fair*
- A protocol(in the real world) is said to be rationally fair if following the protocol is a **computational Nash equilibrium for all the parties**(assumed to be PPT)
- This is a very natural definition
- If a protocol is rationally fair, then no rational PPT party has any incentive to deviate from the protocol (it gains only negligibly in its expected utility)

# Summary in 2 party setting

- Recall that Asharov et al. show a negative result in this context
- However, in their setting, as mentioned, computing the function even in the ideal world is **not a strict Nash equilibrium**
- This is precisely the sufficient condition which is lacking in their setting
- This work shows that if for a given $f$, given distribution $D$ of inputs, and given utility functions, computing $f$ in the ideal world is a strict Nash equilibrium, then there exists a rationally fair protocol in the real world computing $f$ with correctness $1-\text{negl}$
- This protocol is with respect to the same $D$ and the same utility functions
- This result holds in both the fail stop and byzantine settings
- In fail stop setting, parties can either give the correct input or abort
- In byzantine setting, parties can change their input also

# Summary in multiparty setting

- In the multiparty setting, there are $k$ parties, upto $t$ of them might be corrupt and they can collude
- Trivial observation: If the $t, k$ are such that completely fair computation for $t$ malicious parties is possible, then the problem of rationally fair computation is also solved
- So, only those $t, k$ are considered for which completely fair computation with $t$ malicious parties is not possible
- Each party has its own utility function
- This work shows that if for a given $f$, given distribution $D$ of inputs, and given utility functions, computing $f$ in the ideal world is a strict Nash equilibrium for all coalitions of size at most $t$, then there exists a rationally fair protocol in the real world for all coalitions of size at most $t$ computing $f$ with correctness $1-\text{negl}$

# Outline

# The Model

- Let $f : X_1 \times X_2 \times \cdots \times X_k \to Y_1 \times Y_2 \times \cdots \times Y_k$
- Parties $P_1, P_2, \cdots, P_k$ want to compute $f$ on the inputs $x_1, x_2, x_3, \cdots, x_k$
- Output for $P_i$ is $f_i$
- Inputs $x_1, ..x_k$ are chosen according to some joint probability distribution $D$ known to all parties
- Let $x_i$ denote the true inputs, $x_i'$ denote the inputs sent in the protocol, let $y_i'$ denote the outputs obtained in the protocol and $y_i$ denote the final outputs
- Utility functions are defined over the $x_i$ and the $y_i$
- WLOG utilities are non negative
- Let $C$ be a subset of $[k]$
- Then the coaition is $\{P_i : i \in C\}$
- $\bar{C}$ is the complement of $C$
- Honest parties are $\{P_i : i \in \bar{C}\}$

- Let $x_C[i]$ denote the input of party $P_i$ where $i \in C$
- Let $x_C = \{x_C[i] : i \in C\}$
- $x'_C, y'_C, y_C$ are defined similarly
- Utility of a coalition is defined as the sum of the utilities of the individual parties in the coalition
- A coalition can be viewed as being under the control of a centralized adversary

# Ideal World

In the ideal world, the protocol proceeds as follows:

1. Inputs $x_1, \ldots, x_k$ are sampled according to a joint probability distribution $D$, and $x_i$ is then given to $P_i$.
2. Each party sends a value to the trusted party. We also allow parties to send a special value $\perp$ denoting an abort. Let $x_i'$ denote the value sent by $P_i$.
3. If any $x_i' = \perp$, the trusted party sends $\perp$ to all parties. Otherwise, the trusted party sends $f_i(x_1', \ldots, x_k')$ to each party $P_i$.
4. Each party $P_i$ outputs some value $y_i$ which need not be equal to the value it received from the trusted party.

- In the fail stop setting, $x_i' \in \{x_i, \perp\}$
- In Byzantine setting $x_i$ can be anything from $X_i$
- $f_i = y_i'$
- $y_i$ is the value outputted which need not be $y_i'$

# Honest Strategy

- Let $W_i$ be a function from $X_i$ to a distribution over $Y_i$, for all $i \in [k]$
- Honest strategy for party $P_i$ is denoted by (cooperate, $W_i$)
- It is defined as:

> $P_i$ sends its input $x_i$ to the trusted party. If the trusted party returns anything other than $\perp$, then $P_i$ outputs that value. If instead $\perp$ is returned, then $P_i$ generates output according to the distribution $W_i(x_i)$.

- The ideal world protocol is said to be executed honestly by all parties if all parties follow the strategy (cooperate, $W_i$)

# t-resilient strict Nash Equlibrium

This notion is defined for honest execution of the ideal world protocol, that is when all parties follow the strategy (cooperate, $W_i$).
An ideal world protocol(executed honestly) is said to be a **t-resilient strict Nash Equlibrium** if:

1. For every coalition $\mathcal{C}$ of size at most $t$, every (allowed[6]) deviation by the members of $\mathcal{C}$ does not increase the expected utility of $\mathcal{C}$.
2. Moreover, for every coalition $\mathcal{C}$ of size at most $t$, every (allowed) deviation by the members of $\mathcal{C}$ that has $x'_{\mathcal{C}} \neq x_{\mathcal{C}}$ with nonzero probability results in *strictly lower* expected utility for $\mathcal{C}$.

The definition is very natural

# t-Incentive Compatible

Now we can define what it means for an ideal world protocol to be t-incentive compatible

**Definition 1.** *Fix $f$, a distribution $D$, and utility functions $\{U_i\}_{i=1}^k$. We say these are* t-incentive compatible in the fail-stop (resp., Byzantine) setting *if there exist $\{W_i\}_{i=1}^k$ such that the strategy profile $\Big((\text{cooperate}, W_1), \ldots, (\text{cooperate}, W_k)\Big)$ is a t-resilient, Bayesian, strict Nash equilibrium in the ideal-world game defined above.*

As we will see later, the ideal world protocol being t-incentive compatible is the sufficient condition for getting rationally fair real world protocol

**Remark:** It is easy to see that the setting in Asharov et. al is not 1-incentive compatible

# Real world

- No trusted party in the real world
- Rest of the terminology and notation remains same as in the ideal world case
- Assume broadcast channel and secure communication channel between each pair of parties(these are standard assumptions)
- Objective is to get a real world protocol which is rationally fair
- Security parameter is $n$
- All parties have running time polynomial in $n$
- Protocols must have correctness with all but negligible probability in $n$
- Fail Stop setting- Parties can abort the protocol anytime, but it must use the true input and must follow the protocol otherwise(can output anything)
- Byzantine setting- Parties can do whatever feels rational, including changing their input

# t-resilient computational Nash Equilibrium

We had defined rationally fair protocol as a protocol which is a computational Nash Equilibrium when all parties follow the protocol.
A protocol is said to induce a $t-$resilient computational Nash Equilibrium if:

- Any allowed deviation by a coalition C of at most $t$ probabilistic polynomial-time parties yields expected utility at most negligibly more than what C could have obtained by running the protocol honestly and outputting the correct value
- That is, deviating from the protocol cannot increase the expected utility of a coalition of size at most $t$ by more than a negligible amount

# t-Rational

Now that we have the formal definition of computational Nash Equilibrium, we can define what is meant by a rationally fair protocol formally

**Definition 2.** *Fix $f$, a distribution $D$, utilities for the parties, and a protocol $\Pi$ computing $f$. We say $\Pi$ is a* $t$-rational protocol *(with respect to these parameters)* in the fail-stop (resp., Byzantine) setting *if running $\Pi$ is a $t$-resilient, Bayesian, computational Nash equilibrium in the real-world game defined above.*

So a protocol is $t-$rational if it induces a t-resilient computatonal Nash Equilibrium

**Remark:** The parameters are important as the same protocol could be rational with respect to some parameters but may not be rational with respect to other parameters

# Outline

# Protocol structure

- The aim is to get a $t-$rational protocol in the real world from a $t-$incentive compatible protocol in the ideal world
- The protocol **will run in 2 stages**
- The first stage will rely on a secure MPC protocol for a particular functionality(MPC protocol can be unfair)
- Second stage itself has $n$ iterations, in which the output of stage 1 will be useful
- There is a output determination stage as well which comes into play in case abort happens or the protocol terminates successfully

# Stage-1

1. A value $r^* \in \{1, \ldots\}$ is chosen according to a geometric distribution. This represents the iteration (unknown to the parties) in which all parties will learn the correct output.
2. Values $\{(t_1^r, \ldots, t_k^r)\}_{r=1}^n$ are chosen, with $t_i^r$ the value that $P_i$ should learn in iteration $r$. For $r \geq r^*$ we have $t_i^r = f_i(x_1, \ldots, x_k)$, while for $r < r^*$ the value $t_i^r$ depends on $P_i$'s input only

3. Each $t_i^r$ value is shared in a $k$ out of $k$ manner

That is, all the $k$ shares of $t_i^r$ are needed to reconstruct $t_i^r$

# Stage-2

**Second stage:** In each iteration $r \in \{1, \ldots, n\}$, for every $i \in \{1, \ldots, k\}$ each party other than $P_i$ broadcasts its share of $t_i^r$, thus allowing (only) $P_i$ to reconstruct $t_i^r$. When the protocol ends (either through successful termination or an abort by the other party) each party $P_i$ outputs the most-recently-learned value $t_i^r$.

It is clear that stage 2 relies on the output of stage 1(the shares of the $t_i^r$)

# Why it works?

- We already have a ideal world protocol which is a strict Nash equilibrium
- Intuitively, to get a real world protocol with no trusted mediator and satisfying almost same type of equilibrium; **we should try to keep the real world protocol as close as possible to the ideal world protocol** (only modifying whatever is necessary)
- In the ideal world, if mediator outputs abort, parties decide their output according to $W_i(x_i)$
- And in the real world the parties outputs $t_i^r$ for most recent $r$
- In the protocol, for large enough $r$, $t_i^r$ is the true value $f_i$
- For lower values of $r$, $t_i^r$ is sampled according to $W_i(x_i)$
- So in case of early abort **the output of the real world and the output of the ideal world have the same distribution**
- And inputs are anyway from same distribution $D$ for both worlds
- Thus, intuitively, both the protocols should have same equilibrium

# Outline

# The functionality in Stage 1

The functionality needed in Stage 1 is called ShareGen

**Functionality** ShareGen

**Inputs:** ShareGen takes as input a value $x_i$ from each $P_i$.

**Computation:** Proceed as follows:

1. If any $x_i$ input is invalid, then output $\perp$ to all parties.
2. Choose $r^*$ according to a geometric distribution with parameter $p$.
3. Set the values of $t_i^r$ for every $r \in \{1, \ldots, n\}$ and every $i \in \{1, \ldots, k\}$ as follows:
   - If $r < r^*$, choose $t_i^r \leftarrow W_i(x_i)$.
   - If $r \geq r^*$, set $t_i^r = f_i(x_1, \ldots, x_k)$.
4. For each $t_i^r$, choose values $s_{i,j}^r$ as random $k$-out-of-$k$ secret shares of $t_i^r$. I.e., the $\{s_{i,j}^r\}_{j=1}^k$ are chosen uniformly subject to $\bigoplus_{j=1}^k s_{i,j}^r = t_i^r$.

**Output:** Send $P_j$ the values $s_{i,j}^r$ for all $i$ and $r$.

A MPC protocol is needed for implementing this functionality. **The MPC protocol can be any general protocol as long as it is secure against $t$ fail stop adversaries**.

ShareGen is parameterized by a parameter $p$ which is a constant and is determined in the proof.

# The protocol

The protocol uses the functionality ShareGen as a building block

**Protocol Π**

**Stage one:** Parties execute a secure protocol for computing ShareGen. This results in each party $P_j$ obtaining output $s^r_{i,j}$ for $1 \leq i \leq k$ and $1 \leq r \leq n$. (If ShareGen returns $\perp$, go to the output-determination phase.)

**Stage two:** There are $n$ iterations. In each iteration $r \in \{1, \ldots, n\}$ do:

- Each $P_j$ broadcasts $\{s^r_{i,j}\}_{i \neq j}$.
- If some party does not broadcast a value, go to the output-determination phase. Otherwise, each $P_j$ computes $t^r_j = \bigoplus_{i=1}^{k} s^r_{j,i}$.

**Output determination:** Each party $P_j$ determines its output as follows:

- If an abort occurs before $P_j$ has computed $t^1_j$, then $P_j$ chooses its output according to distribution $W_j(x_j)$.
- If an abort occurs at any other point, or the protocol completes successfully, then $P_i$ outputs the last $t^r_i$ value it computed.

As mentioned, this protocol can use any MPC protocol for computing ShareGen that is secure against $t$ fail stop adversaries with unanimous abort

# Main Theorem

Having described the protocol, now we come to the main theorem which says that $t-$ incentive compatible implies $t-$rational

**Theorem 1.** *Fix a function $f$, a distribution $D$, and utilities for the parties. If these are $t$-incentive compatible in the fail-stop setting, then (assuming the existence of general secure multiparty computation for $t$ fail-stop adversaries) there exists a protocol $\Pi$ computing $f$ such that $\Pi$ is a $t$-rational protocol (with respect to the same distribution and utilities) in the fail-stop setting.*

Since the adversary is fail-stop, it is possible to analyze $\Pi$ in a **hybrid world** where there is a trusted entity computing the functionality ShareGen instead of the MPC protocol.
Since the MPC protocol for ShareGen has unanimous abort but not necessarily fairness, the trusted entity computing ShareGen in the hybrid world doesn't have fairness necessarily but all honest parties abort together
**If $\Pi$ is a computational Nash equilibrium in this hybrid world, then it is also so when executed in the real world where the** ShareGen **is computed by the secure MPC protocol instead of the trusted entity**

# Outline

# A preliminary lemma

The proof of the main theorem uses a preliminary lemma.
Before that a definition:
**Distribution with complete support:** A distribution over a finite set $S$ is said to have complete support over $T \subset S$ if it gives a non zero probability to every element of $S$.
Following this definition, we can define what it means for $W_i$ to have **full support**
$W_i$ **with full support**- $W_i : X_i \to D(Y_i)$ is said to have full support if for all $x_i \in X_i$, the distribution $W_i(x_i) \in D(Y_i)$ has complete support over $f_i(X_1 \times \cdots \times X_k)$
The lemma is as follows:

**Lemma 3.** *Fix a function $f$, a distribution $D$, and utilities for the parties that are t-incentive compatible in the fail-stop (resp., Byzantine) setting. Then there exist $\{W_i\}$* **with full support** *such that $\Big((\text{cooperate}, W_1), \ldots, (\text{cooperate}, W_k)\Big)$ is a t-resilient, Bayesian, strict Nash equilibrium in the fail-stop (resp., Byzantine) setting.*

# Proof of the Lemma

Steps in the proof:

- Incentive compatibility gives us $W_1', W_2', \cdots, W_k'$ where these may not necessarily have full support
- Define $u_{\max}$ as the maximum utility possible for any coalition of size at most $t$
- Fix a coalition determined by $C \subset [k]$
- Let $u(x_C)$ denote the expected utility of coalition determined by $C$ if it behaves honestly, that is if $P_i$ follows the strategy (cooperate, $W_i$) for all $i \in C$
- Let $u_\perp(x_C)$ denote the maximum expected utility of coalition determined by $C$ if it aborts
- Let $u^*$ be the minimum of $u(x_C) - u_\perp(x_C)$ where minimum is over all $C$ and all true input values $x_C$
- By incentive compatibility, $u^* > 0$
- Let $\epsilon = \frac{u^*}{2k \cdot u_{\max}}$
- The distribution $W_i(x_i)$ is defined to be $W_i'(x_i)$ with probability $1 - \epsilon$ and $U(f_i(X_1 \times \cdots \times X_k))$ with probability $1 - \epsilon$
- This definition is for all $i \in [k]$
- Clearly $W_i$ have full support
- It can also be shown that the corresponding strategy profile is a $t-$resilient strict Nash Equilibrium

# Some remarks

- Recall that the protocol uses the functionality ShareGen as a building block. ShareGen uses a constant $p$ as a parameter
- Since $p$ is a parameter for the geometric distribution, $r^* \leq n$ with all but negligible probability
- Thus, when all parties are honest, they get the correct output with all but negligible probability
- It is also possible to redefine $r^*$ so that correctness is guaranteed
- The goal is to show that there exists a $p > 0$ for which the protocol described is a $t-$rational protocol in the hybrid model with respect to the given parameters(which are $t-$incentive compatible)
- That is, fix an arbitrary coalition determined by $C$ of cardinality at most $t$
- We need to show that no fail stop deviation by this coalition can increase the utility of the coalition by more than a negligible amount

# Some modifications(WLOG)

For the proof, the protocol is modified in the following 2 ways:

- At the beginning of each iteration the coalition is informed whether the current iteration $r > r^*$ or not
- If any party in the coalition aborts in iteration $r \leq r^*$, the coalition is informed whether $r = r^*$ before the output determination stage
- This is without loss of generality as all these modifications can only increase the incentive for the coalition to deviate as it might get higher utility by deviating than in the unmodified protocol
- So, **it suffices to prove the $t-$rationality of the modified protocol(in the hybrid world)**

# Proof Part 1

- Note that once $r > r^*$, there is no incentive for the parties in the coalition to deviate at all
- This is because if $r > r^*$, all parties have got the correct outputs
- So, this is effectively the ideal world case where all parties have got the correct outputs from the trusted party
- Since by assumption, in the ideal world the corrupt parties(in the coalition) won't benefit by changing their output from what they received, they won't benefit in this case either
- So we only need to consider $r \leq r^*$
- When proving the lemma, we defined $u(x_C)$ to be the utility of $C$ when following the ideal world protocol honestly
- Now suppose $C$ follows the real world protocol honestly, let utility in this case be $u'(x_C)$
- Then, it is easy to see that $u(x_C) = u'(x_C)$(as inputs and outputs are same)
- Let $u_\perp(x_C)$ be as before(in ideal world)
- Define $u^*$ as the minimum of $u(x_C) - u_\perp(x_C)$ where minimum is over all possible coalitions of size at most $t$ and over all true inputs
- Then,we have $u^* > 0$
- Let $t_C^r = \{t_i^r; i \in C\}$
- It is the values that the parties in the coalition learn in the $r^{\text{th}}$ iteration

# Proof Part 2

- If parties in $C$ never abort, they get utility $u(x_C)$
- If they decide to abort in some iteration $r$, then as $r \leq r^*$, they are told with probability $\alpha$ that $r = r^*$ and with probability $1 - \alpha$ that $r < r^*$
- If they are informed that $r = r^*$, then at most they can get utility $u_{\max}$ and if they are told that $r < r^*$ then they get utility at most $u_\perp(x_C)$ (as the parties in $C$ know nothing more than they knew in ideal world)
- So expected utility of aborting is at most

$$\alpha \cdot u_{\max} + (1 - \alpha) \cdot u_\perp(x_C)$$

  which is less than $u(x_C)$(the honest utility) for $\alpha \leq \frac{u^*}{u_{\max}}$
- So if $\alpha \leq \frac{u^*}{u_{\max}}$, then the expected utility of abort is at most the expected utility of honestly following the protocol
- So it suffices to show that we can find $p$ such that $\alpha \leq \frac{u^*}{u_{\max}}$ holds for all $x_C, t_C^r$

# Proof Part 3

Let $q = \min_{x_C, t_C}\{\Pr[\forall P_i \in \mathcal{C} : W_i(x_i) = t_i]\}$. Since the $\{W_i\}$ have full support, $q > 0$. Now, for any coalition $\mathcal{C}$ given inputs $x_C$ and observing outputs $t_C$ in some iteration $r \leq r^*$, we have

$$
\begin{aligned}
\alpha &\stackrel{\text{def}}{=} \Pr[r^* = r \mid t_C^r = t_C \wedge r^* \geq r] \\
&= \frac{\Pr[r^* = r \wedge t_C^r = t_C \mid r^* \geq r]}{\Pr[t_C^r = t_C \mid r^* \geq r]} \\
&= \frac{\Pr[r^* = r \mid r^* \geq r] \cdot \Pr[t_C^r = t_C \mid r^* = r]}{\Pr[r^* = r \mid r^* \geq r] \cdot \Pr[t_C^r = t_C \mid r^* = r] + \Pr[r^* > r \mid r^* \geq r] \cdot \Pr[t_C^r = t_C \mid r^* > r]} \\
&= \frac{p \cdot \Pr[t_C^r = t_C \mid r^* = r]}{p \cdot \Pr[t_C^r = t_C \mid r^* = r] + (1-p) \cdot \Pr[t_C^r = t_C \mid r^* > r]} \\
&\leq \frac{p}{p + (1-p) \cdot q} \\
&= \frac{p}{p \cdot (1-q) + q} \leq \frac{p}{q}.
\end{aligned}
$$

Note that $q$ is a positive constant and so if we choose $p$ such that $p = \frac{u^* \cdot q}{u_{\max}}$, we get the required upper bound on $\alpha$

So, this completes the proof.

**Remark**-This argument works for $r < n$. In case of $r = n$, aborting will give higher expected utility to $C$(for $r \leq r^*$). But this happens with negligible probability(hence computational Nash Equilibrium)

Also, this protocol is private. The parties only learn the output that they are supposed to learn and nothing else

# Outline

# Some Remarks for the Byzantine case

- It is possible to modify the protocol to make it work in the Byzantine case
- The assumption will be that the ideal world protocol is $t-$incentive compatible in case of byzantine deviations
- Mainly, the ShareGen functionality must be modified so that all the shares are authenticated
- So, the functionality ShareGen will generate public/private key pair for a secure digital signature scheme and will sign each share(concatenated with iteration number and party index) given to each party using the private key
- And the public key will be an output of the functionality
- Whenever the honest parties will receive shares, they need to verify the signature and that the iteration number and party index is what it should be
- If verification fails then parties should abort
- The ShareGen functionality can be implemented using a general MPC protocol secure against $t$ malicious parties with unanimous abort

# Theorem in the Byzantine Case

The theorem is as follows:

**Theorem 2.** *If a function $f$, a distribution $D$, and utilities for the parties are $t$-incentive compatible in the Byzantine setting, then (assuming the existence of digital signatures and general secure multiparty computation for $t$ malicious adversaries) there exists a protocol $\Pi$ computing $f$ that is a $t$-rational protocol (with respect to the same distribution and utilities) in the Byzantine setting.*

# Outline

# Questions that remain

- Positive results were shown assuming strict Nash Equilibrium. Can positive results be shown assuming weaker kind of equilibrium?
- The real world protocol constructed induces a computational Nash Equilibrium. Can protocols be constructed inducing stronger equilibrium notions without increasing the assumptions?
- Is a converse of the result in this work possible? If we get an equilibrium in the real world with no trusted mediator, can we get a stronger notion of equilibrium in the ideal world by introducing a mediator?

*Thank you!*