A Complete Characterization of Game-Theoretically Fair, Multi-Party Coin Toss

Gilad Asharov, Elaine Shi, and Ke Wu
What to eat for crypto seminar?

Sushi!

Cake!
[Blum 83]
[Blum 83]
Coin toss protocol

- **Correctness**: if all honest, output is uniformly random.

- **Strong fairness**: strategic player cannot bias the output. ❌

Impossible due to [Cle86]
Coin toss protocol

- **Correctness**: if all honest, output is uniformly random.

- **Game-theoretic fairness**: strategic player cannot benefit herself.
Game-theoretic fair $n$-party coin toss?

Coalition

Utility = \begin{cases} 1, & \text{if I like output} \\ 0, & \text{otherwise} \end{cases}
Multi-party coin toss protocol

- **Correctness**: if all honest, output is uniformly random.

- **Game-theoretic fairness**: a coalition cannot increase its expected utility.

Honest protocol is a Nash equilibrium!
Why we care?

**Strong fairness** is impossible if half sized coalition.

Want fairness against majority sized coalition.
Game-theoretic fair $n$-party coin toss?

Sushi!

Cake!

Impossible against $(n - 1)$-coalition due to [CGL+18].
Smaller coalition

? Game-theoretic fair $n$-party coin toss against $< n - 1$?

Yes!
A strawman solution

Sushi!

Cake!
Sushi!

No preference

Cake!
Sushi!

Cake!

Cannot benefit
Sushi!

Cake!

Cannot tolerate coalition of size 3
Under what size of coalition is it possible to achieve game-theoretic fairness?

Feasible region?

\[ \max\left\{ \left\lfloor \frac{n}{2} \right\rfloor - 1, 2 \right\} \leq n - 1 \]
Complete characterization

- A game-theoretic fair coin toss against $t$-coalition.

- Game-theoretic fairness is impossible against $(t + 1)$-coalition.
Protocol

Sushi! $s_0$ ⊕ Cake! $s_1$

Outcome
Secret sharing trusted authority

- Only $\geq k$ players can ask to reveal $s$.
- Any $\geq k$ players can rewrite $s$.

$k$-

$\$ s
Reveal $s = 0$

Reveal

$2-$

$\frac{\$}{s} = 0$
\[ s = 0 \]
2- \text{Bank} \quad s = 0

s = 1
Only rewrite once before any reveal request.
Summary of trusted authority

- Only $\geq k$ players can ask to reveal $s$.
- Any $\geq k$ players can rewrite $s$ before reveal;
Our protocol

\[
\text{Output } s_0 \oplus s_1
\]

\[
\begin{array}{c}
\square \quad s_0 \quad s_1 \quad \square \\
\end{array}
\]

Reveal

Reveal

Reveal

Reveal

Reveal

Reveal

Reveal
Output $s_0$?

- $s_0$
- $s_0$
- $s_1$

Reveal

- $s_0$
- $s_0$
- $s_1$

Reveal

- $s_0$
- $s_0$
- $s_1$

Reveal
Output 0!

\[
\begin{array}{c}
\square \quad S_0 \quad \square \quad \square \\
\end{array}
\]
Asymmetric

Why is this protocol asymmetric?
Output $s_1$

$2^- \quad \text{Reveal} \quad s_0$

$\text{Reveal} \quad \text{Reveal} \quad \text{Reveal} \quad \text{Reveal}$
Output 0!

Reveal $s_0$

Reveal $s_1$

Reveal
Fairness against coalition of size 4

No preference
Output $s_1$

$2- s$

$\textcircled{\$} s_0$

$\textcircled{\$} s_1$

2-
Output $s_0 \oplus s_1$

$s_0$

$s_1$

2-
Output 0!

2-s

Reveal

Reveal

Reveal

Reveal

$S_0$

$S_1$
This protocol is game-theoretic fair again coalition of size 4.

Can we generalize?

<table>
<thead>
<tr>
<th>Achievability</th>
<th>Coalition size $t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n_1 \geq \frac{5}{2}n_0$</td>
<td>$n_1 - \frac{1}{2}n_0$</td>
</tr>
<tr>
<td>otherwise</td>
<td>$\frac{2}{3}n_1 + \frac{1}{3}n_0$</td>
</tr>
</tbody>
</table>

Game-theoretic fairness is impossible against $(t + 1)$-coalition.
Landscape
Phase Transition

<table>
<thead>
<tr>
<th>Achievability</th>
<th>Coalition size $t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>( if \ n_1 \geq \frac{5}{2}n_0 )</td>
<td>( n_1 - \frac{1}{2}n_0 )</td>
</tr>
<tr>
<td>\textit{otherwise}</td>
<td>( \frac{2}{3}n_1 + \frac{1}{3}n_0 )</td>
</tr>
</tbody>
</table>
Output $0!$

$S_0$

$2-\text{ Sushi}$

$2-\text{ Cake}$

$S_0$

$S_1$

$\text{People}$
Output 0!

\[ \begin{array}{c}
\square \quad S_0 \quad \square \quad \square \\
\end{array} \]

\[ S_0 \quad \quad 2- \quad \quad \$
\]

\[ S_0 \quad \quad 2- \quad \quad \$
\]

\[ S_1 \]
How to choose the threshold in general?
Sushi!

Cake!
• **Condition 1**: Coalition cannot control both coins.

\[ k_0 - \text{\[\text{pillows}\]} \]

\[ \text{\[\$\]} s_0 \]

\[ k_1 - \text{\[\text{cake}\]} \]

\[ \text{\[\$\]} s_1 \]

\[ t \leq k_0 + k_1 \]
• **Condition 2:** If control $s_1$, cannot fail reconstruction of $s_0$.

\[ t \leq (n_0 - k_0 + 1) + k_1 \]
• **Condition 3**: If can fail reconstruction of $s_1$, must not prefer $0$.

$$k_0 \leq 1 - s_0$$

$$k_1 \leq 1 - s_1$$

$$\text{If } n_1 - k_1 < n_0, \; t \leq 2(n_1 - k_1)$$
Achievability: optimization

Maximize $t$

Subject to $t < (k_0 + 1) + (k_1 + 1)$

$t < (n_0 - k_0) + (k_1 + 1)$

If $n_1 - k_1 < n_0$, $t \leq 2(n_1 - k_1)$

<table>
<thead>
<tr>
<th></th>
<th>$k_0$</th>
<th>$k_1$</th>
<th>$t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n_1 \geq \frac{5}{2}n_0$</td>
<td>$\frac{1}{2}n_0$</td>
<td>$n_1 - n_0$</td>
<td>$n_1 - \frac{1}{2}n_0$</td>
</tr>
<tr>
<td>otherwise</td>
<td>$\frac{1}{2}n_0$</td>
<td>$\frac{2}{3}n_1 - \frac{1}{6}n_0$</td>
<td>$\frac{2}{3}n_1 + \frac{1}{3}n_0$</td>
</tr>
</tbody>
</table>
Three conditions imply fairness

- **Condition 1**: Coalition cannot control both coins.

- **Condition 2**: If control $s_1$, cannot fail reconstruction of $s_0$.

- **Condition 3**: If can fail reconstruction of $s_1$, must not prefer 0.
Conclusion

1. We can construct game-theoretic fair coin toss against coalition of size

\[
t = \begin{cases} 
   n_1 - \left\lfloor \frac{1}{2} n_0 \right\rfloor, & \text{if } n_1 \geq \frac{5}{2} n_0, \\
   \left\lfloor \frac{1}{2} n_0 \right\rfloor + \left\lfloor \frac{2}{3} n_1 - \frac{1}{6} n_0 \right\rfloor, & \text{otherwise.}
\end{cases}
\]

2. There is no game-theoretic fair coin toss against \((t + 1)\)-sized coalition.
1. Complete characterization of another fairness notion: no coalition can harm honest individual.

2. Complete characterization under other utility.
[Cle 86] Richard Cleve. *Limits on the security of coin flips when half the processors are faulty*. In STOC, 1986.
