TEL AVIV UNIVERSITY

An (Almost) Optimally Fair 3-Party Coin-Flipping

Iftach Haitner and Eliad Tsfadia

TCE Summer School on Computer Security

September 2014

Coin-Flipping Protocols

I want $c = 0$

Parties want to jointly flip a uniform bit

B 

$c \leftarrow \{0,1\}$

$\xleftarrow{\quad 0 \quad}$

Output c

Blum's Coin-Flipping Protocol

Negligible bias

B 

 A

$z \leftarrow commit(a)$

$a \leftarrow \{0,1\}$

b

$b \leftarrow \{0,1\}$

$a \leftarrow decommit(z)$

Output: $a \oplus b$

A **cheats or aborts**: B aborts.

If Honest Party Must output a Bit

Bias ¼

B 

 A

$z \leftarrow commit(a)$ $\qquad a \leftarrow \{0,1\}$

$b \leftarrow \{0,1\}$ $\qquad b$

$a \leftarrow decommit(\boldsymbol{z})$

Output: $a \oplus b$

A **cheats or aborts**: B outputs some bit

2-Party Coin-Flipping Protocols

Efficient 2-party protocol (A,B) is δ-bias CF:

1. $\Pr[(\mathrm{A,B})(1^n) = 0] = \Pr[(\mathrm{A,B})(1^n) = 1] = {}^1\!/_2$
2. For any PPT $\mathcal{A}^*$ and bit c:

$$\Pr[(\mathcal{A}^*,\mathrm{B})(1^n) = c] \leq {}^1\!/_2 + \delta(n)$$

(Same for B)

❖ **Honest party must output a bit.**

[Cleve '86]: Any m-round 2-party CF protocol can be biased by $\Omega\left(\frac{1}{m}\right)$

$\Longrightarrow$ m-round $\Theta\left(\frac{1}{m}\right)$-bias CF is called optimally fair.

Many-Party Coin-Flipping Protocols

A t-party δ-bias CF is analogously defined.

1. In honest execution, parties output common uniform bit.
2. Even if some parties cheats, honest parties output **common** δ-close to uniform bit.

- Negative results for 2-party protocols applied to many-party case.
- Positive results for many-party protocols seem harder to get than in the 2-party case.

❖ We focus on the 3-party case.

Known Results (positive)

- [Blum '82]: $\frac{1}{4}$-bias CF.
- [Cleve '86]: m-round 2-party $\Theta\left(\frac{1}{\sqrt{m}}\right)$-bias CF.
  - Both results assume One-Way Functions (OWFs)
  - Both can be extended to the multiparty case.

- [Moran, Naor, Segev '09]: m-round 2-party $\Theta\left(\frac{1}{m}\right)$-bias CF
- [Beimel, Omri, Orlov '11]: m-round t-party $\Theta\left(\frac{1}{m}\right)$-bias CF, against $\ell < \frac{2}{3} \cdot t$ corrupted parties.
  - Both results assume Oblivious Transfer (OT).

- For $\frac{2}{3}$ or more corrupted parties [Cleve '86] was the best known protocol.

Known Results (negative)

- [Cleve '86]: Any m-round 2-party CF protocol can be biased by $\Omega\left(\frac{1}{m}\right)$.

Holds in any computational model.

- [Cleve, Impagliazzo '93] - In the fail-stop model, any m-round 2-party CF protocol can be biased by $\Omega\left(\frac{1}{\sqrt{m}}\right)$.

  fail-stop model: parties are unbounded, and their only malicious action is abort prematurely.

In the random oracle model:

- [Soled et. al '11]: No $m \in o\left(\frac{n}{\log(n)}\right)$-round 2-party optimally fair CF, where n is oracle input length.
- [Soled et. al '14]: No oblivious 2-party optimally fair CF protocol.

- [Berman, Haitner, Tentes' 14]:
  CF (even "unfair") of any constant bias implies OWF.

Our Result

Theorem:

Assuming *Oblivious Transfer*,

there exists m-round, 3-party $O(\frac{\log^2 m}{m})$-bias CF.

Construction outline:

- New 2-party $O(\frac{\log^2 m}{m})$-bias CF
  - Builds upon Cleve's majority protocol
  - Does not use *threshold round paradigm*, used in [MNS '09] and [BOO '11]
- 3-party CF using the new 2-party CF.

Why Optimally-Fair Coin Flipping?

- Fundamental and natural primitive
- Step towards general optimally-fair SFE

Cleve’s 2-Party Majority Protocol

Cleve's 2-Party Protocol

This is $\Theta\left(\frac{1}{\sqrt{m}}\right)$-bias CF protocol

B

For $i = 1$ to m:

A

$z \leftarrow commit(a_i)$ $a_i \leftarrow \{-1,1\}$

$b_i \leftarrow \{-1,1\}$ b_i

$a_i \leftarrow decommit(z)$

$\boxed{c_i = a_i \cdot b_i}$

Output: $\mathrm{Sign}(\sum_{i=1}^{m} c_i)$.

A **aborts at round** i: B chooses uniform $c_i, \dots, c_m$ by itself.

Analysis

B

For $i = 1$ to m:

$\mathcal{A}^*$

By aborting, $\mathcal{A}^*$ "gains" the difference between (protocol) expected outcome, and B's expected output in case of **abort**

$$z \leftarrow commit(a_{\mathrm{i}}) \qquad a_{\mathrm{i}} \leftarrow \{-1,1\}$$

$$\mathrm{b_i} \leftarrow \{-1,1\} \qquad \mathrm{b_i}$$

$$a_{\mathrm{i}} \leftarrow decommit(z)$$

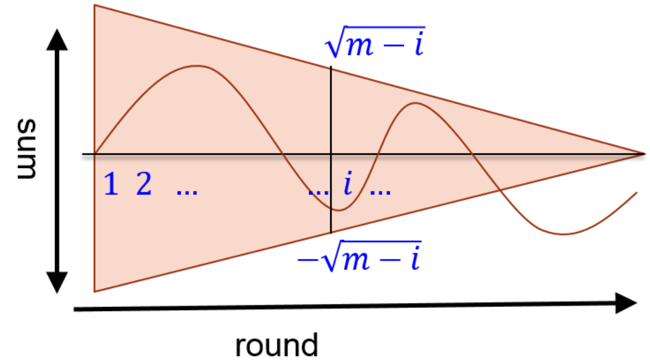
$$\mathrm{c_i} = a_{\mathrm{i}} \cdot \mathrm{b_i}$$

Output: $\mathrm{Sign}(\sum_{i=1}^{m} c_i)$.

A **aborts at round** i: B chooses uniform $c_i, \dots, c_m$ by itself.

Analysis, cont.

$S_k = \sum_{j=1}^{k} c_j \approx N(0,k) \approx$ uniform over $[-\sqrt{k}, \sqrt{k}\,]$



- $|S_{i-1}| > \sqrt{m-i}$: abort at round i gains nothing
- $|S_{i-1}| \leq \sqrt{m-i}$: abort at round i gains bias $\frac{1}{\sqrt{m-i}}$

  ($\Pr[S_m \in \{-1,1\}]$ conditioned on $|S_{i-1}| \leq \sqrt{m-i}$)

- $\Pr\left[|S_{i-1}| \leq \sqrt{m-i}\right] = \frac{\sqrt{m-i}}{\sqrt{m}}$ (for $i \in \Omega(m)$)

On average: abort at round i gains bias $\frac{\sqrt{m-i}}{\sqrt{m}} \cdot \frac{1}{\sqrt{m-i}} = \frac{1}{\sqrt{m}}$

Our 2-Party Protocol

Unfairness in Cleve's Protocol

B 

For $i = 1$ to m:

 A

$\frac{1}{\sqrt{m}}$ difference between expected outcome, and B's expected output

$z \leftarrow commit(a_i)$ ← $a_i \leftarrow \{-1,1\}$

$b_i \leftarrow \{-1,1\}$ → b_i

$a_i \leftarrow decommit(z)$ ←

$\boxed{c_i = a_i \cdot b_i}$

Output: $\mathrm{Sign}(\sum_{i=1}^{m} c_i)$.

A **aborts at round** i: B chooses uniform $c_i, \ldots, c_m$ by itself.

Where does B get the sample from?
Now B can bias A's outcome…

B

For $i = 1$ to m:

A

B gets sample according to expected outcome at end of round i

$z \leftarrow commit(a_{\mathrm{i}})$ $\quad a_{\mathrm{i}} \leftarrow \{-1,1\}$

$\mathrm{b}_{\mathrm{i}} \leftarrow \{-1,1\}$ $\quad \mathrm{b}_{\mathrm{i}}$

$a_{\mathrm{i}} \leftarrow decommit(z)$

$\mathrm{c}_{\mathrm{i}} = a_{\mathrm{i}} \cdot \mathrm{b}_{\mathrm{i}}$

Output: $\mathrm{Sign}(\sum_{i=1}^{m} c_i)$.
A **aborts at round** i: B outputs the (i-1)'th sample.

The (Non-fair) Dealer Paradigm

Construct CF by 2-phase protocol:

1. Honest, non-fair dealer outputs shares to the parties.
   - Non-fair – Rushing adversary gets its shares first and might abort (preventing the other party from getting its shares)
2. Parties use shares as auxiliary input for their interaction.

- Parties are fail-stop – follow the protocol but might abort.

Assuming oblivious transfer,

δ-bias CF in this model $\Longrightarrow$ δ-bias CF in the standard model.

Cleve's Protocol Using Dealer Paradigm

1. For $i = 1$ to m:
   $c_i \leftarrow \{-1,1\}$.
2. Split $\{c_i\}_{i=1}^{m}$ into two sets of shares using 2-out-of-2 Secret Sharing Scheme (SSS).

B's shares of $\{c_i\}_{i=1}^{m}$

A's shares of $\{c_i\}_{i=1}^{m}$

B

A

For $i = 1$ to m:

B sends his share of c_i

A sends her share of c_i

Both parties reconstruct c_i

Output: $\mathrm{Sign}(\sum_{i=1}^{m} c_i)$.

A aborts at round i: B chooses uniform $c_i, \dots, c_m$ by itself.

Our 2-Party Protocol, the Dealer

Dealer:

1. For $i = 1$ to m:
   a) $c_i \leftarrow \{-1,1\}$
   b) $\boxed{\delta_i = \Pr\left[\sum_{j=1}^{m} c_j \geq 0 | c_1, \ldots, c_i\right]}$
   c) $\boxed{d_i^A, d_i^B \leftarrow Ber(\delta_i)}$, (1 w.p. δ_i and 0 o/w)

2. Split $\left\{\boxed{d_i^A, d_i^B}, c_i\right\}_{i=1}^{m}$ into two sets of shares using 2-out-of-2 SSS

- δ_i is protocol expected outcome given $c_1, \ldots, c_i$.

We call $\{d_i^A, d_i^B\}$ the "defense values"

- d_i^A and d_i^B are sampled according to δ_i – expected outcome at end of round (i, b)

$\Longrightarrow$ aborting at step (i,b) is harmless.

- d_i^A and d_i^B leaks only limited information about δ_i (and c_i).

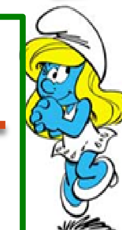
$\Longrightarrow$ aborting at step (i,a) is not "too harmful"

For $i = 1$ to m:

B 

(a) B sends his share of d_i^A $\longrightarrow$ $\longleftarrow$ A sends her share of d_i^B

Party P reconstructs d_i^{P}

 A

(b) B sends his share of c_i $\longrightarrow$ $\longleftarrow$ A sends her share of c_i

Both parties reconstruct c_i

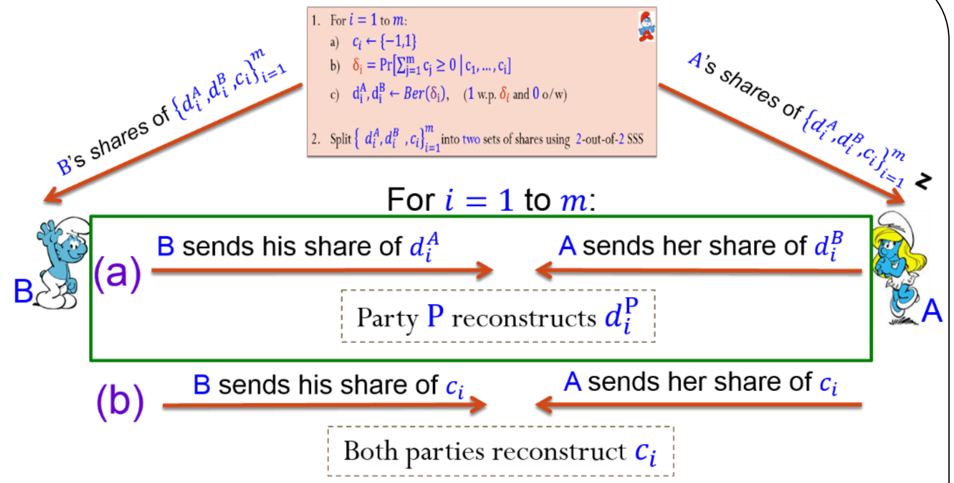
Output: $\mathrm{Sign}(\sum_{i=1}^{m} c_i)$.

A aborts at round (i, a): B outputs d_{i-1}^B (uniform bit if $i = 1$)

A aborts at round (i, b): B outputs d_i^B

Analysis

d_i^A and d_i^B are sampled according to expected outcome at end of round (i, b)



Output: $\mathrm{Sign}(\sum_{i=1}^{m} c_i)$.
A aborts at round $(i$,a): B outputs d_{i-1}^B (uniform bit if $i = 1$)
A aborts at round $(i$,b): B outputs d_i^B

Aborting at round $(i$,b) is harmless

Aborting at round $(i$,a):

$S_k = \sum_{i=1}^{k} c_j \approx$ uni. over $[-\sqrt{k}, \sqrt{k}\,]$

Compare to $\frac{1}{\sqrt{m-i}}$ in Cleve

- $|S_{i-1}| > \sqrt{m-i}$: abort at round i, gives nothing
- $|S_{i-1}| \leq \sqrt{m-i}$: abort at round i, yields bias $\frac{1}{m-i}$

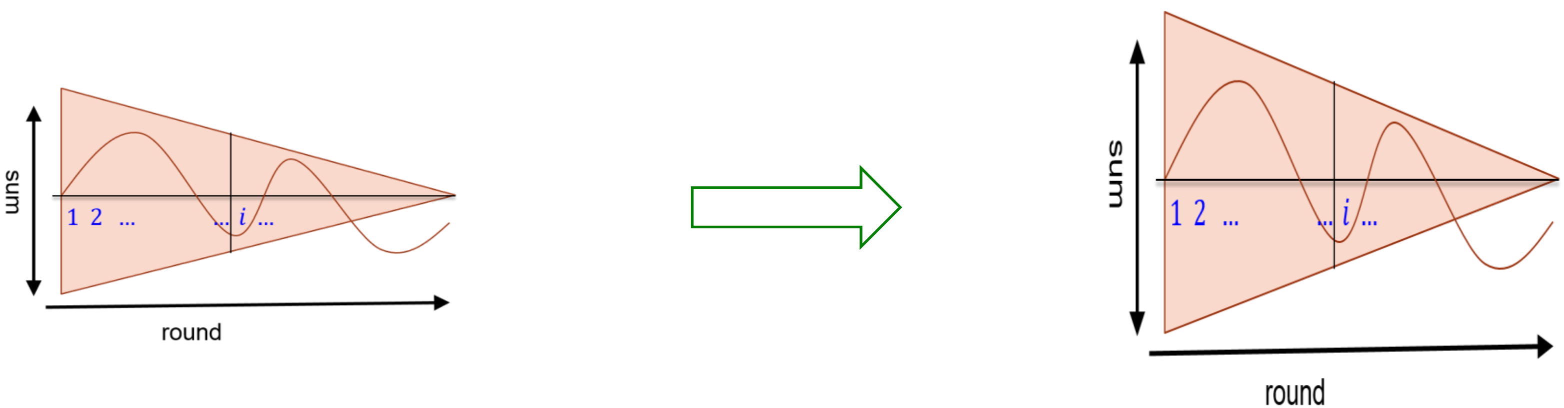
On average: abort at round j achieves bias $\frac{\sqrt{m-i}}{\sqrt{m}} \cdot \frac{1}{m-i} = \frac{1}{\sqrt{m(m-i)}}$

$\Theta\left(\frac{1}{m}\right)$ for "small" i (e.g., $i = 1$), but $\Theta\left(\frac{1}{\sqrt{m}}\right)$ for "large" i (e.g., $i = m$)

Weighted Majority Protocol

First rounds get larger influence

m	m-1	...	3	2	1
c_1	c_2	...	c_{m-2}	c_{m-1}	c_m



- Aborting at round (i,a) yields bias $\Theta\left(\frac{1}{m}\right)$, for any i
- Since $\mathcal{A}^*$ might be adaptive, additional $\log\ m$ factor is paid.

Our 3-Party Protocol

3-Party Coin-Flipping (reminder)

Efficient 3-party protocol $(\mathrm{A},\mathrm{B},\mathrm{C})$ is δ-bias CF:

1. $\Pr[(\mathrm{A},\mathrm{B},\mathrm{C})(1^n) = 0] = \Pr[(\mathrm{A},\mathrm{B},\mathrm{C})(1^n) = 1] = 1/2$
2. For any PPTs $\mathcal{A}^*$ and B^*, and bit c:

$$\Pr[(\mathcal{A}^*, B^*, \mathrm{C})(1^n) = c] \leq 1/2 + \delta(n)$$

(Same for other two-party collations)

- Non-aborting parties must output the **same** bit.

Unfairness in 3-party Cleve

For $i = 1$ to m:

$\frac{1}{\sqrt{m}}$ difference between expected outcome and (B,C)'s expected output

A

$a_{\mathrm{i}} \leftarrow \{-1,1\}$

B

$\mathrm{b_i} \leftarrow \{-1,1\}$

C

$\mathrm{e_i} \leftarrow \{-1,1\}$

commit(b_i)

decommit

commit(a_{i})

decommit

commit($\mathrm{e_i}$)

decommit

Broadcast Channel

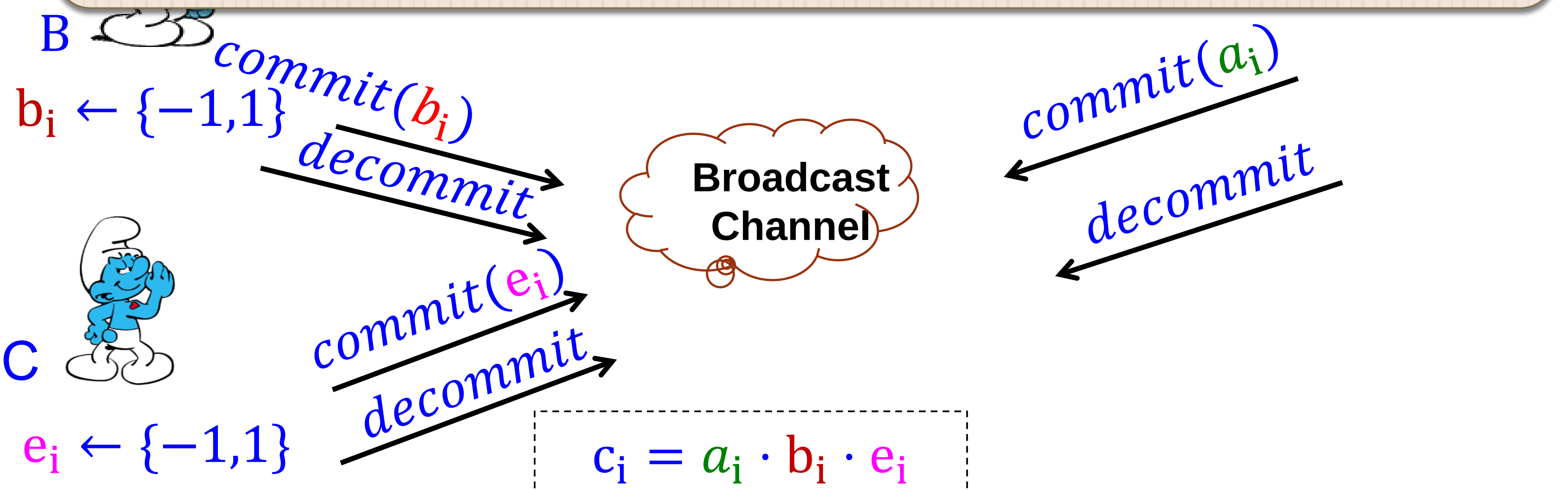
$\mathrm{c_i} = a_{\mathrm{i}} \cdot \mathrm{b_i} \cdot \mathrm{e_i}$

Output: $\mathrm{Sign}(\sum_{i=1}^{m} c_i)$.

A **aborts at round** i: (B,C) chooses $c_i, \ldots, c_m$ by themselves.

Use hiding 2-party dealer that leaks limited information about expected outcome

(B,C) get shares for 2-party **sub-protocol**, whose outcome is sampled according to expected outcome at end of round i



Output: $\mathrm{Sign}(\sum_{i=1}^{m} c_i)$.

A **aborts at round** i: (B,C) chooses $c_i, \dots, c_m$ by themselves.

Hiding Dealer

D is a parameterized dealer, if:

$D(\gamma, m)$ outputs shares of m-round $\tilde{O}\left(\frac{1}{m}\right)$-bias 2-party CF, with expected outcome γ (i.e., 1 w.p. γ and 0 o/w).

D is hiding if: $SD\Big(D(\alpha, m), D(\alpha + \Delta)\Big) \in \Theta(\Delta)$

$D(\gamma, m)$ does not leak more information about γ than a γ-biased coin

A variant of our 2-party dealer is a parameterized hiding dealer for $\Delta \in o(1)$

Such dealer suffices, since underlying Cleve protocol is "smooth"

Our 3-Party Protocol

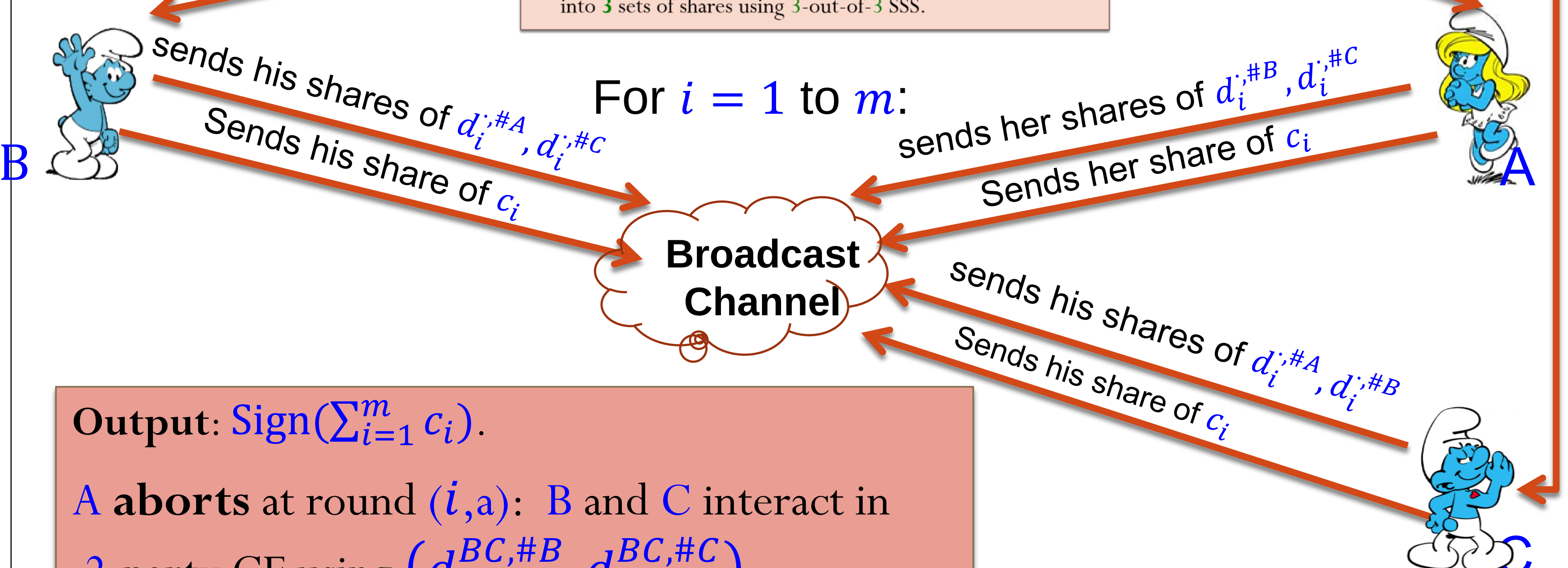
Dealer:

D − parameterized hiding dealer for m-round, 2-party $\tilde{O}\left(\frac{1}{m}\right)$-bias CF

1. For $i = 1$ to m:
   a) $c_i \leftarrow \{-1,1\}$
   b) Let $\delta_i = \Pr\left[\sum_{j=1}^{m} c_j \geq 0 \,\middle|\, c_1, \dots, c_i\right]$.
   c) $(d_i^{AB,\#A}, d_i^{AB,\#B}),\ (d_i^{AC,\#A}, d_i^{AC,\#C}),\ (d_i^{BC,\#B}, d_i^{BC,\#C}) \leftarrow D(\delta_i, m)$
2. Split $\{d_i^{AB,\#A}, d_i^{AB,\#B}, d_i^{AC,\#A}, d_i^{AC,\#C}, d_i^{BC,\#B}, d_i^{BC,\#C}, c_i\}_{i=1}^{m}$ into **3** sets of shares using 3-out-of-3 SSS.

Our 3-Party Protocol

1. For $i = 1$ to m:
   a) $c_i \leftarrow \{-1,1\}$
   b) Let $\delta_i = \Pr\left[\sum_{j=1}^{m} c_j \geq 0 \mid c_1, \ldots, c_i\right]$.
   c) $(d_i^{AB,\#A}, d_i^{AB,\#B}),\ (d_i^{AC,\#A}, d_i^{AC,\#C}),\ (d_i^{BC,\#B}, d_i^{BC,\#C}) \leftarrow D(\delta_i, m)$
2. Split $\{d_i^{AB,\#A}, d_i^{AB,\#B}, d_i^{AC,\#A}, d_i^{AC,\#C}, d_i^{BC,\#B}, d_i^{BC,\#C}, c_i\}_{i=1}^{m}$ into 3 sets of shares using 3-out-of-3 SSS.



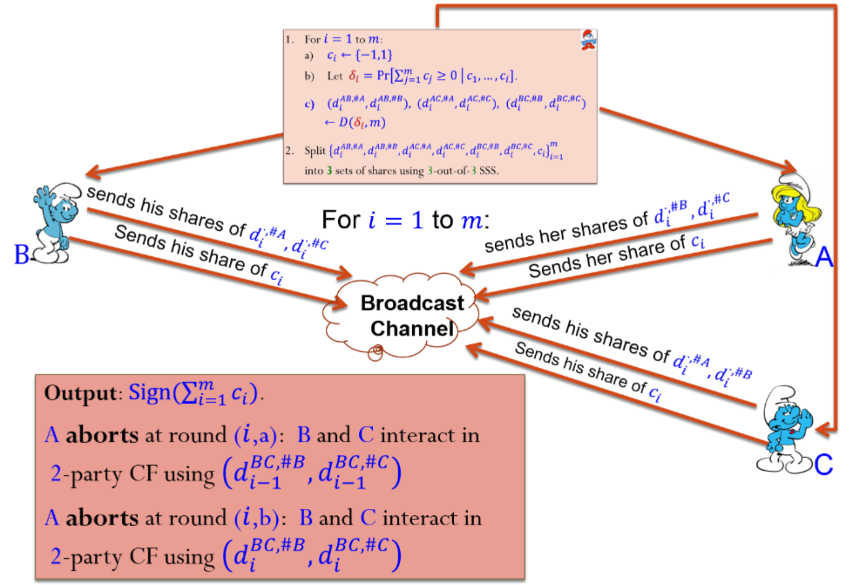
Output: $\mathrm{Sign}\left(\sum_{i=1}^{m} c_i\right)$.

A **aborts** at round (i,a): B and C interact in 2-party CF using $\left(d_{i-1}^{BC,\#B}, d_{i-1}^{BC,\#C}\right)$

A **aborts** at round (i,b): B and C interact in 2-party CF using $\left(d_{i}^{BC,\#B}, d_{i}^{BC,\#C}\right)$

Analysis

1. For $i = 1$ to m:
   a) $c_i \leftarrow \{-1,1\}$
   b) Let $\delta_i = \Pr[\sum_{j=1}^{m} c_j \geq 0 \mid c_1, \ldots, c_i]$.
   c) $(d_i^{AB,\#A}, d_i^{AB,\#B})$, $(d_i^{AC,\#A}, d_i^{AC,\#C})$, $(d_i^{BC,\#B}, d_i^{BC,\#C})$ $\leftarrow D(\delta_i, m)$
2. Split $\{d_i^{AB,\#A}, d_i^{AB,\#B}, d_i^{AC,\#A}, d_i^{AC,\#C}, d_i^{BC,\#B}, d_i^{BC,\#C}, c_i\}_{i=1}^{m}$ into **3** sets of shares using 3-out-of-3 SSS.



$\mathcal{A}^*$ and $\mathcal{B}^*$ wants to bias the protocol using 2 aborts.

- $D(\delta_i, m)$ hides $\delta_i \Longrightarrow$ First abort achieves $\tilde{O}\left(\frac{1}{m}\right)$ bias.
- $D(\delta_i, m)$ is $\tilde{O}\left(\frac{1}{m}\right)$-bias CF $\Longrightarrow$ Second abort achieves $\tilde{O}\left(\frac{1}{m}\right)$ bias.

2-Party Hiding Dealer

Hiding Dealer (reminder)

D is a parameterized dealer, if:

D(γ,m) outputs shares of m-round $\tilde{O}\left(\frac{1}{m}\right)$-bias 2-party CF,
with expected outcome γ (i.e., 1 w.p. γ and 0 o/w).

D is hiding if: $SD\big(D(\alpha, m), D(\alpha + \Delta)\big) \in \Theta(\Delta)$

Non-Hiding Dealer

- C_ϵ – distribution over $\{-1,1\}$, taking 1 w.p. $\frac{1}{2}+\epsilon$ and -1 o/w.

Input: γ:

1. Set $\epsilon = (\gamma - \frac{1}{2})/\sqrt{m}$ $\qquad \left(\Pr_{(c_1,\ldots,c_m)\leftarrow(C_\epsilon)^m}[\sum_{i=1}^m c_i \geq 0] = \gamma\right)$
2. For $i = 1$ to m, let
   a) $c_i \leftarrow C_\epsilon$
   b) $\delta_i = \Pr\left[\sum_{j=1}^m c_j \geq 0 \,\middle|\, c_1, \ldots, c_i\right]$
   c) $d_i^A, d_i^B \leftarrow Ber(\delta_i)$
3. Split $\left\{d_i^A, d_i^B, c_i\right\}_{i=1}^m$ into two sets of shares using 2-out-of-2 secret sharing scheme

Effectively, $\{d_i^A, d_i^B\}_{i=1}^m$ form 2m independent samples from $Ber(\gamma)$, and thus determine γ.

Hiding Dealer

- C_ϵ – dist. over $\{-1,1\}$, taking 1 w.p. $\frac{1}{2}+\epsilon$ and -1 o/w.

Input: γ

1. Set $\epsilon = (\gamma - \frac{1}{2})/\sqrt{\mathrm{m}}$

$\boxed{\text{Let } S \leftarrow (C_\epsilon)^{2m}}$

2. For $i = 1$ to m, let
   a) $c_i \leftarrow C_\epsilon$
   b) $\delta_i = \Pr\left[\sum_{j=1}^{m} c_j \geq 0 \,\middle|\, c_1, \ldots, c_i\right]$
   c) $d_i^A, d_i^B \leftarrow Ber(\delta_i)$

3. Sp … haring sch…

$Ber(\delta_i)$: $\mathrm{Sign}\left(\sum_{j=1}^{i} c_j + \sum_{c \in S_{m-i}} c\right)$

where S_{m-i} is a random subset of S of size m-i

- Only 2m samples from C_ϵ
- $SD\big(D(\alpha, m), D(\alpha+\Delta)\big) \in \Theta(\Delta)$, for $\Delta \in o(1)$
- Proving fairness is harder

Open Problems

- Removing the $O(\log^2 m)$ factor
- More than 3 parties
- Necessity of Oblivious Transfer
- Applications to fair SFE