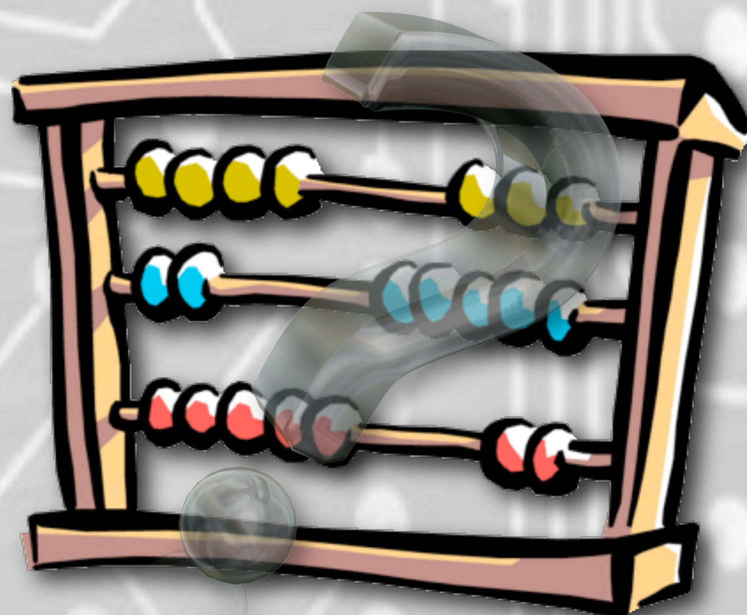
The Computational Complexity of Coin Flipping



Hemanta K. Maji
Manoj Prabhakaran
Amit Sahai

Weak Coin [Blum82]

Weak Coin [Blum82]

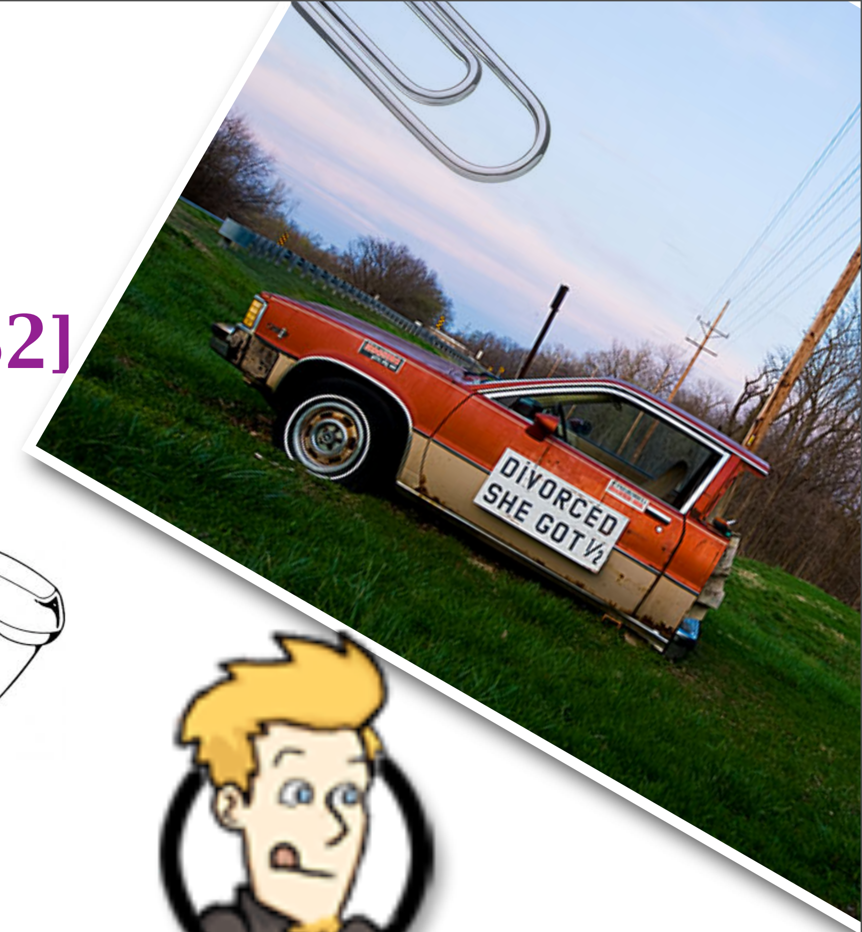
Weak Coin [Blum82]

Weak Coin [Blum82]

Weak Coin [Blum82]

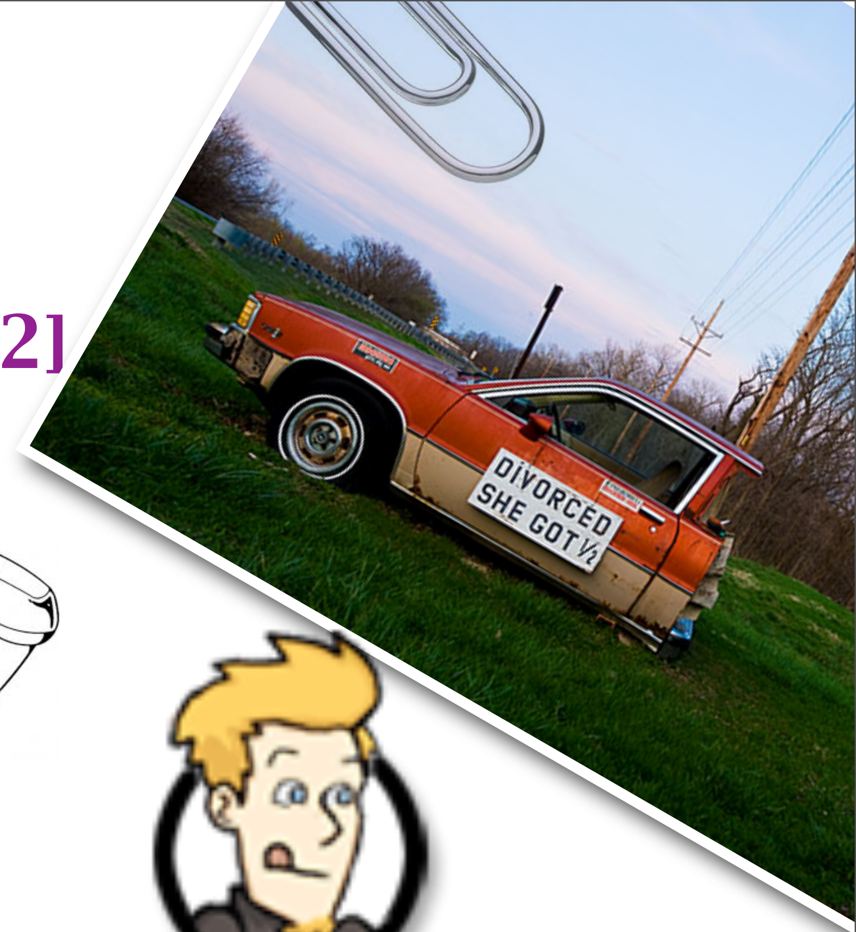
Who gets the car?

Weak Coin [Blum82]



Who gets the car?

Weak Coin [Blum82]



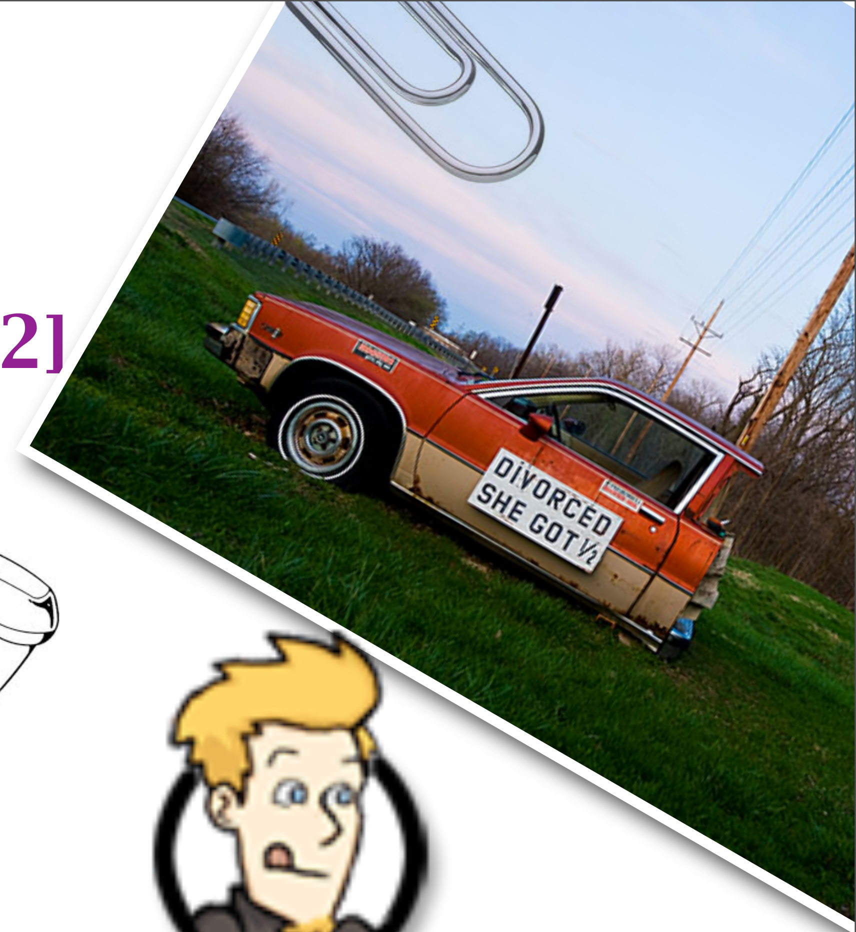
Who gets the car?

Weak Coin [Blum82]

Who gets the car?

if the outcome is

Weak Coin [Blum82]



Who gets the car?

Alice gets the car
if the outcome is

Weak Coin [Blum82]

Who gets the car?

Alice gets the car
if the outcome is

Bob gets the car
if the outcome is

Weak Coin

Weak Coin

- Original problem introduced in [Blum82]

Weak Coin

- Original problem introduced in [Blum82]
- Definition: Alice wants Heads; Bob wants Tails

Weak Coin

- Original problem introduced in [BLUM82]
- Definition: Alice wants Heads; Bob wants Tails
  - When Alice and Bob interact honestly the probability of Heads = $^1/_2$

Weak Coin

- Original problem introduced in **[Blum82]**
- Definition: Alice wants Heads; Bob wants Tails
  - When Alice and Bob interact honestly the probability of Heads = $^1/_2$
  - Probability of a Dishonest player's preferred outcome is not "*significantly*" higher than $^1/_2$ when the other player plays honestly

Weak Coin

- Original problem introduced in **[Blum82]**
- Definition: Alice wants Heads; Bob wants Tails
  - When Alice and Bob interact honestly the probability of Heads = $^1/_2$
  - Probability of a Dishonest player's preferred outcome is not "*significantly*" higher than $^1/_2$ when the other player plays honestly
- Aim: Understand computational intractability required for a weak coin tossing protocol

Definition

Definition

- Security Parameter: k

Definition

- Security Parameter: k
- Corresponding protocol: $\pi(k)$

Definition

- Security Parameter: k
- Corresponding protocol: $\pi(k)$
- Security Guarantee: $\mu(k)$ in the range $[0,1]$

Definition

- Security Parameter: k
- Corresponding protocol: $\pi(k)$
- Security Guarantee: $\mu(k)$ in the range $[0,1]$
  - Neither party can get their preferred outcome with probability more than $1 - \mu(k)/2$

Definition

- Security Parameter: k
- Corresponding protocol: $\pi(k)$
- Security Guarantee: $\mu(k)$ in the range $[0,1]$
    - Neither party can get their preferred outcome with probability more than $1 - \mu(k)/2$
    - 1 secure protocol: Fully secure

Definition

- Security Parameter: k
- Corresponding protocol: $\pi(k)$
- Security Guarantee: $\mu(k)$ in the range $[0,1]$
  - Neither party can get their preferred outcome with probability more than $1 - \mu(k)/2$
  - 1 secure protocol: Fully secure
  - 0 secure protocol: No security Guarantee

Protocol Models

Protocol Models

- General $\pi(k)$:

Protocol Models

- General $\pi(k)$:
  - k-round protocols

Protocol Models

- General $\pi(k)$:
  - k-round protocols
  - Alice and Bob send bits alternately

Protocol Models

- General $\pi(k)$:
  - k-round protocols
  - Alice and Bob send bits alternately
- Constant Alternation $\pi(k)$:

Protocol Models

- General $\pi(k)$:
  - k-round protocols
  - Alice and Bob send bits alternately
- Constant Alternation $\pi(k)$:
  - Constant number of rounds

Protocol Models

- General $\pi(k)$:
  - k-round protocols
  - Alice and Bob send bits alternately
- Constant Alternation $\pi(k)$:
  - Constant number of rounds
  - Alice and Bob send k-bit messages alternately

Known Results

Known Results

+ OWF implies $1 - \nu$ secure Constant Alternation protocol, for some negligible ν [Blum82, GL89, Naor89, HILL99]

Known Results

+ OWF implies $1 - \nu$ secure Constant Alternation protocol, for some negligible ν [Blum82, GL89, Naor89, HILL99]

• Alice commits to a

Known Results

+ OWF implies $1 - \nu$ secure Constant Alternation protocol, for some negligible ν [Blum82, GL89, Naor89, HILL99]

- Alice commits to a
- Bob sends b

Known Results

+ OWF implies $1 - \nu$ secure Constant Alternation protocol, for some negligible ν [Blum82, GL89, Naor89, HILL99]

- Alice commits to a
- Bob sends b
- Alice de-commits a and outcome is $a \oplus b$

Known Results

+ OWF implies $1 - \nu$ secure Constant Alternation protocol, for some negligible ν [Blum82, GL89, Naor89, HILL99]

- Alice commits to a
- Bob sends b
- Alice de-commits a and outcome is $a \oplus b$
- If a party aborts, then the outcome is opposite to his/her preferred outcome

Known Results

- OWF implies $1 - \nu$ secure Constant Alternation protocol, for some negligible ν [Blum82, GL89, Naor89, HILL99]

Known Results

+ OWF implies $1 - \nu$ secure Constant Alternation protocol, for some negligible ν [Blum82, GL89, Naor89, HILL99]

- General Protocols:

Known Results

+ OWF implies $1 - \nu$ secure Constant Alternation protocol, for some negligible ν [Blum82, GL89, Naor89, HILL99]

- General Protocols:
    - $^1/_{2^k}$ secure protocols implies PSPACE $\not\subseteq$ BPP

Known Results

+ OWF implies $1 - \nu$ secure Constant Alternation protocol, for some negligible ν [Blum82, GL89, Naor89, HILL99]

- General Protocols:
  - $^1/_{2^k}$ secure protocols implies PSPACE $\not\subseteq$ BPP

Brute Force

Known Results

+ OWF implies $1 - \nu$ secure Constant Alternation protocol, for some negligible ν [Blum82, GL89, Naor89, HILL99]

- General Protocols:

  Brute Force

  - $^1/_{2^k}$ secure protocols implies PSPACE $\not\subseteq$ BPP
  - $1 - \theta(^1/_{\sqrt{k}})$ secure protocols implies OWF [CI93]

Known Results

+ OWF implies $1 - \nu$ secure Constant Alternation protocol, for some negligible ν [Blum82, GL89, Naor89, HILL99]

- General Protocols:

  - $^1/_{2^k}$ secure protocols implies PSPACE $\not\subseteq$ BPP

  - $1 - \theta(^1/_{\sqrt{k}})$ secure protocols implies OWF [CI93]

Brute Force

Martingale Result

Known Results

+ OWF implies $1 - \nu$ secure Constant Alternation protocol, for some negligible ν [BLUM82, GL89, NAOR89, HILL99]

- General Protocols:
  - $^{1}/_{2^k}$ secure protocols implies PSPACE $\not\subseteq$ BPP
  - $1 - \theta(^{1}/_{\sqrt{k}})$ secure protocols implies OWF [CI93]

- Constant Alternation Protocols:

Brute Force

Martingale Result

Known Results

+ OWF implies $1 - \nu$ secure Constant Alternation protocol, for some negligible ν [Blum82, GL89, Naor89, HILL99]

- General Protocols:
  - $^{1}/_{2k}$ secure protocols implies PSPACE $\not\subseteq$ BPP
  - $1 - \theta(^{1}/_{\sqrt{k}})$ secure protocols implies OWF [CI93]

- Constant Alternation Protocols:
  - $^{1}/_{2k}$ secure protocols implies PH $\not\subseteq$ BPP, which implies NP $\not\subseteq$ BPP [Zachos88]

Brute Force

Martingale Result

Known Results

+ OWF implies $1 - \nu$ secure Constant Alternation protocol, for some negligible ν [Blum82, GL89, Naor89, HILL99]

- General Protocols:
  - $^1/_{2^k}$ secure protocols implies PSPACE $\not\subseteq$ BPP
  - $1 - \theta(^1/_{\sqrt{k}})$ secure protocols implies OWF [CI93]

- Constant Alternation Protocols:
  - $^1/_{2^k}$ secure protocols implies PH $\not\subseteq$ BPP, which implies NP $\not\subseteq$ BPP [Zachos88]

Brute Force

Martingale Result

Brute Force

Gaps in Understanding

Gaps in Understanding

- Proposed by [IMPAGLIAZZO09]

Gaps in Understanding

- Proposed by [Impagliazzo09]
- Is it necessary that $P \neq NP$ for existence of a $^{49}/_{50}$ secure weak coin tossing protocol?

Gaps in Understanding

- Proposed by [IMPAGLIAZZO09]
- Is it necessary that $P \neq NP$ for existence of a $^{49}/_{50}$ secure weak coin tossing protocol?
  - Is $P \neq NP$ necessary, if we want to restrict the probability of each party's preferred outcome to at most $^{1}/_{2} + ^{1}/_{100}$?

Gaps in Understanding

- Proposed by **[IMPAGLIAZZO09]**
- Is it necessary that $P \neq NP$ for existence of a $^{49}/_{50}$ secure weak coin tossing protocol?
    - Is $P \neq NP$ necessary, if we want to restrict the probability of each party's preferred outcome to at most $^{1}/_{2} + ^{1}/_{100}$?
- Alternately, if $P = NP$ is there a constant bias attack against General protocols?

Results [MPS10]

Results [MPS10]

- General protocols:

Results [MPS10]

- General protocols:
  - $^1/_2 + {}^1/_{poly}$ secure protocol implies NP $\not\subseteq$ BPP

Results [MPS10]

- General protocols:
  - $^1/_2 + ^1/_{poly}$ secure protocol implies NP $\not\subseteq$ BPP
  - Reworded: NP $\subseteq$ BPP implies some party can force his/her preferred outcome with probability at least $^3/_4 - ^1/_{poly}$

Results [MPS10]

- General protocols:
  - $^1/_2 + {}^1/_{poly}$ secure protocol implies NP $\not\subseteq$ BPP
  - Reworded: NP $\subseteq$ BPP implies some party can force his/her preferred outcome with probability at least $^3/_4 - {}^1/_{poly}$

- Constant Alternation protocols:

Results [MPS10]

- General protocols:
  - $^1/_2 + {^1/_{poly}}$ secure protocol implies $NP \not\subseteq BPP$
  - Reworded: $NP \subseteq BPP$ implies some party can force his/her preferred outcome with probability at least $^3/_4 - {^1/_{poly}}$
- Constant Alternation protocols:
  - $^1/_{poly}$ secure protocol implies OWF

Results [MPS10]

- General protocols:
  - $^1/_2 + {}^1/_{poly}$ secure protocol implies $NP \not\subseteq BPP$
  - Reworded: $NP \subseteq BPP$ implies some party can force his/her preferred outcome with probability at least $^3/_4 - {}^1/_{poly}$

- Constant Alternation protocols:
  - $^1/_{poly}$ secure protocol implies OWF
  - Reworded: $\neg$OWF implies some party can force his/her preferred outcome with probability at least $1 - {}^1/_{poly}$

Results [MPS10]

- General protocols:
  - $^1/_2 + ^1/_{poly}$ secure protocol implies NP $\not\subseteq$ BPP
  - Reworded: NP $\subseteq$ BPP implies some party can force his/her preferred outcome with probability at least $^3/_4 - ^1/_{poly}$

Tight!

- Constant Alternation protocols:
  - $^1/_{poly}$ secure protocol implies OWF
  - Reworded: ¬OWF implies some party can force his/her preferred outcome with probability at least $1 - ^1/_{poly}$

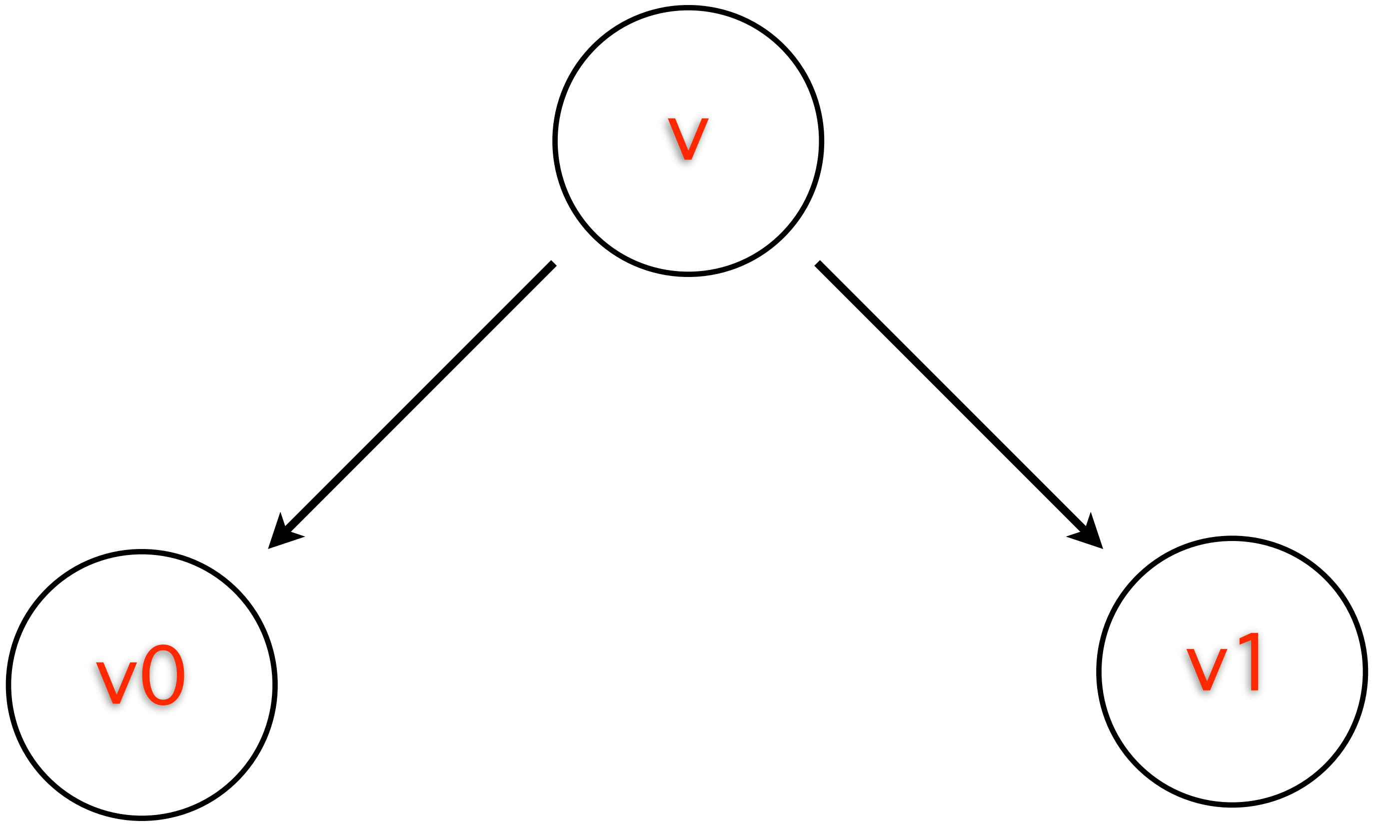
Protocol Tree

Protocol Tree

- Partial transcripts are vertices; v is parent of v0 and v1

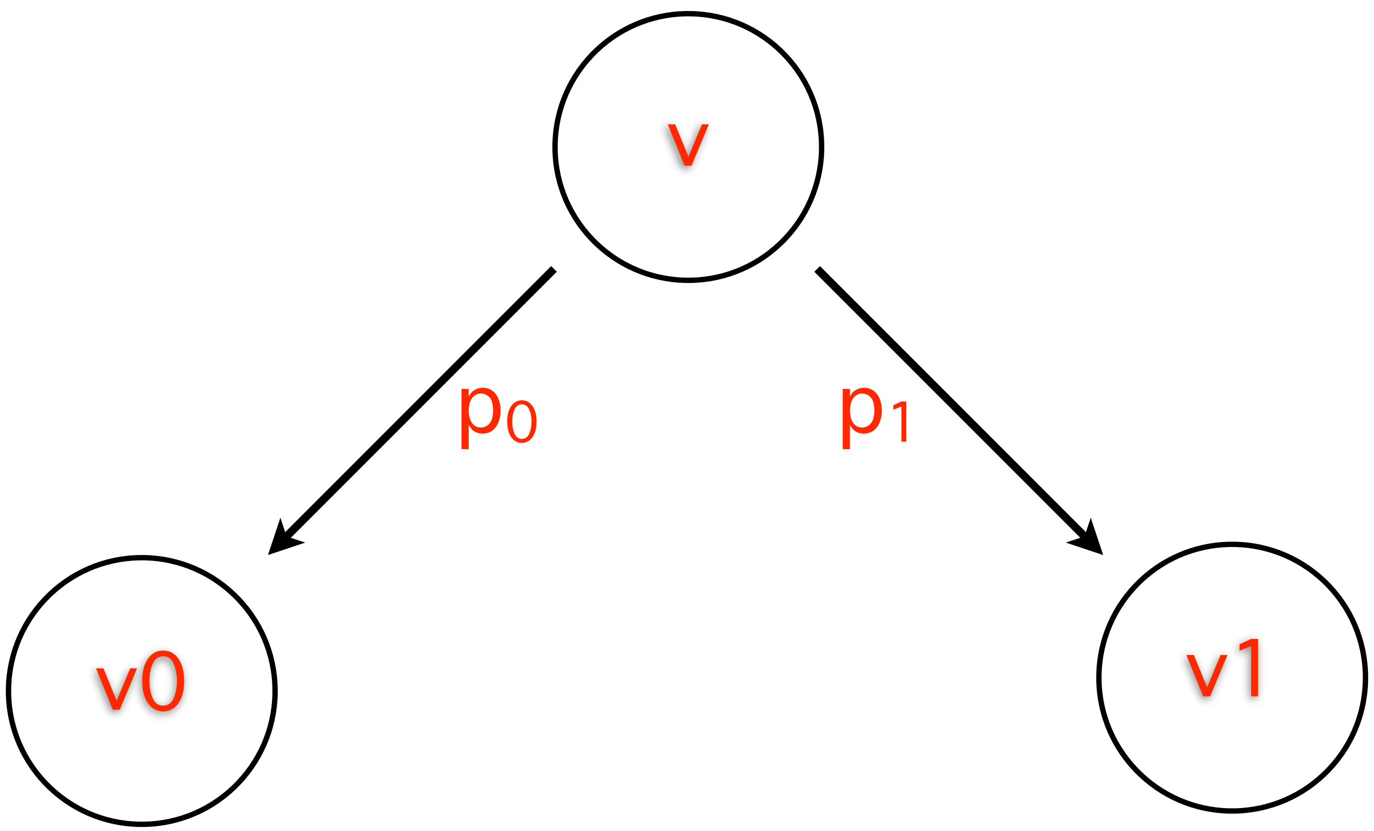
Protocol Tree

- Partial transcripts are vertices; v is parent of v0 and v1



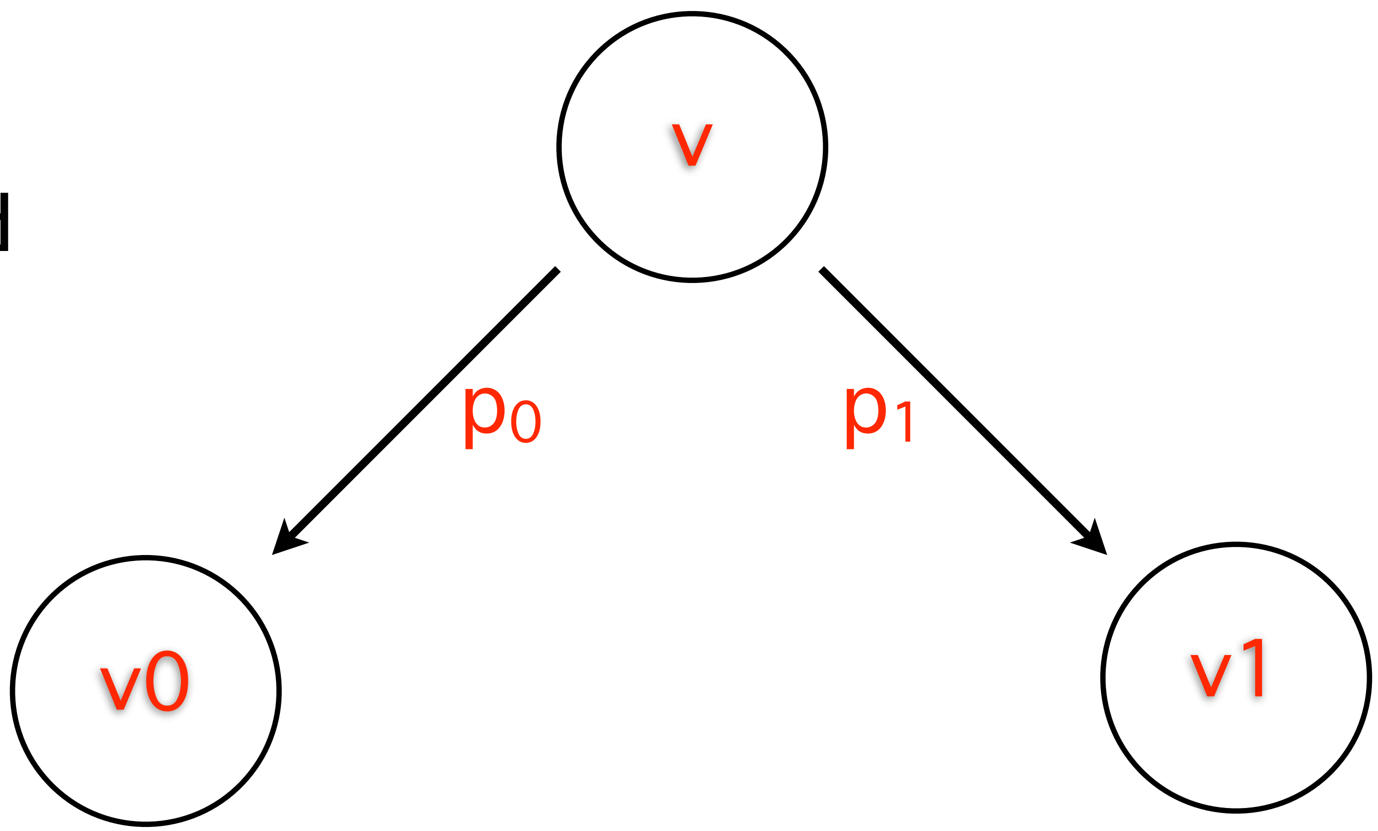
Protocol Tree

- Partial transcripts are vertices; v is parent of v0 and v1



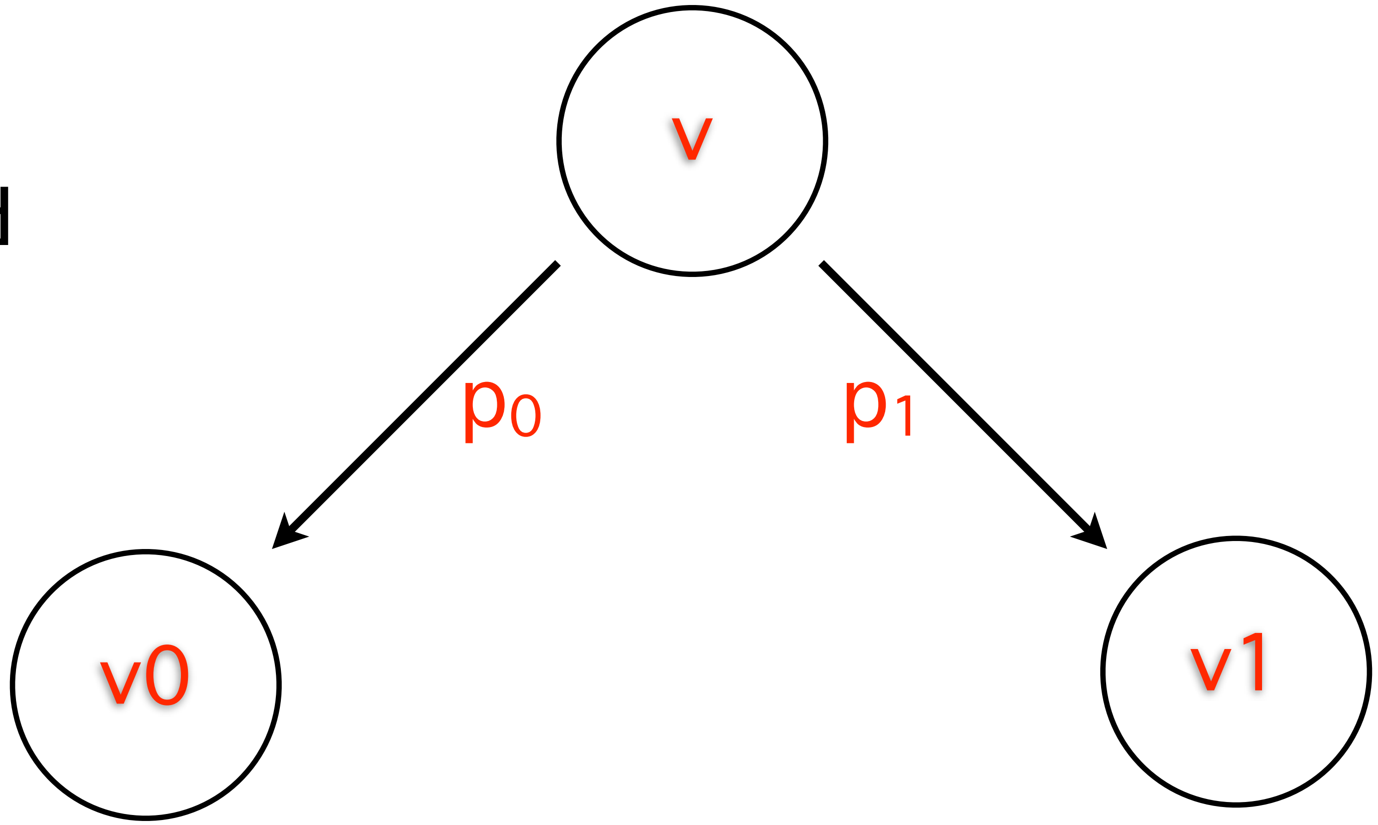
Protocol Tree

- Partial transcripts are vertices; v is parent of v0 and v1
- Interpret Heads as 1 and Tails as 0



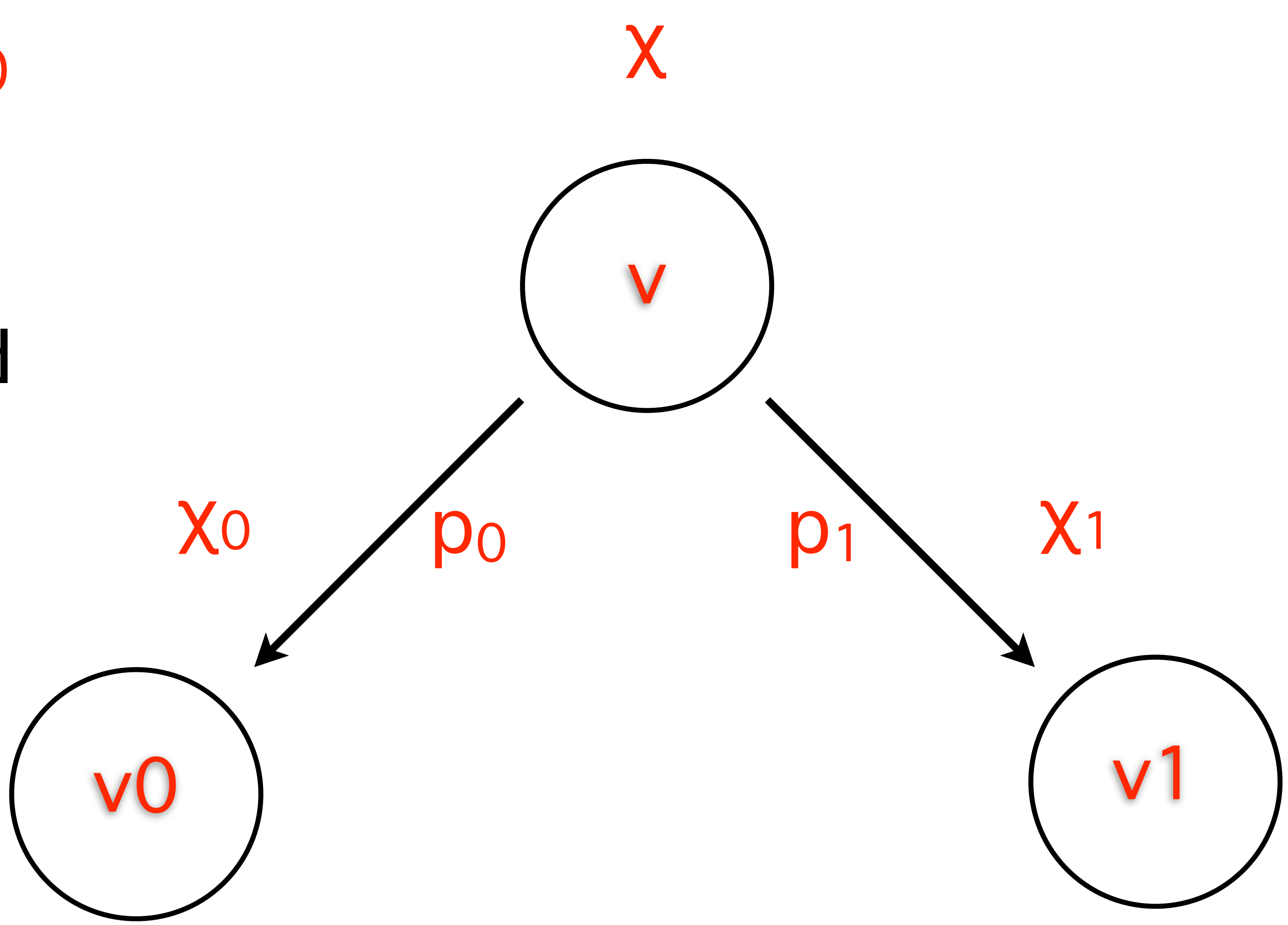
Protocol Tree

- Partial transcripts are vertices; v is parent of v0 and v1
- Interpret Heads as 1 and Tails as 0
- Color of a node v (χ): Expectation of the outcome when both parties behave honestly conditioned on v being the transcript prefix



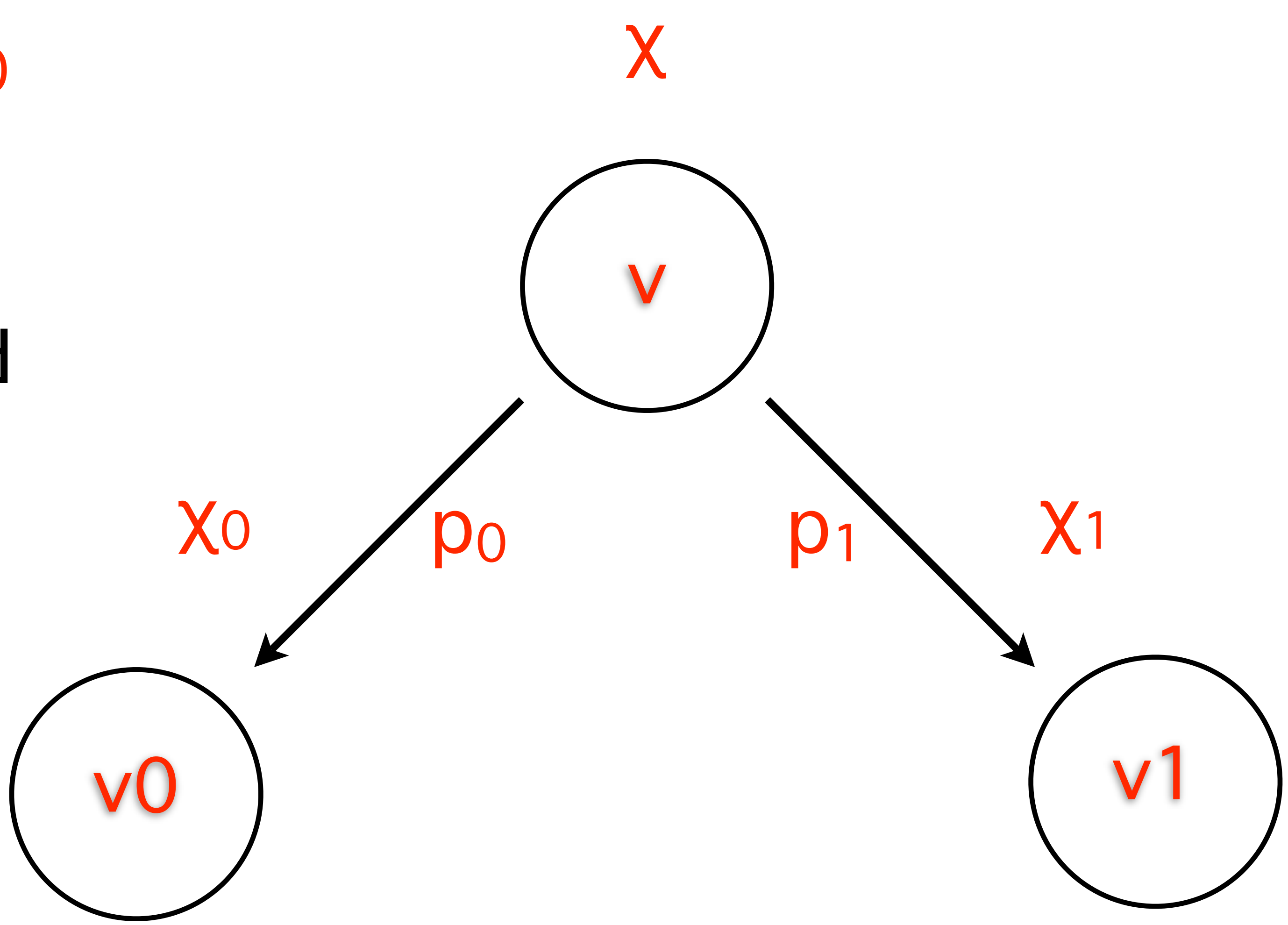
Protocol Tree

- Partial transcripts are vertices; v is parent of v0 and v1
- Interpret Heads as 1 and Tails as 0
- Color of a node v (χ): Expectation of the outcome when both parties behave honestly conditioned on v being the transcript prefix



Protocol Tree

- Partial transcripts are vertices; v is parent of v0 and v1
- Interpret Heads as 1 and Tails as 0
- Color of a node v (χ): Expectation of the outcome when both parties behave honestly conditioned on v being the transcript prefix



$$\chi = p_0\chi_0 + p_1\chi_1$$

Uniform Generation

Uniform Generation

- For NP relations **[JVV86]**:

Uniform Generation

- For NP relations [JVV86]:
  - Uniformly sample from $R^{-1}(x) = \{w \mid R(x; w) = 1\}$

Uniform Generation

- For NP relations **[JVV86]**:
  - Uniformly sample from $R^{-1}(x) = \{w \mid R(x; w) = 1\}$
  - Efficient algorithm using NP Oracle **[BGP00]**

Uniform Generation

- For NP relations **[JVV86]**:
  - Uniformly sample from $R^{-1}(x) = \{w \mid R(x; w) = 1\}$
  - Efficient algorithm using NP Oracle **[BGP00]**
- NP $\subseteq$ BPP implies efficient algorithm

Uniform Generation

- For NP relations **[JVV86]**:
  - Uniformly sample from $R^{-1}(x) = \{w \mid R(x; w) = 1\}$
  - Efficient algorithm using NP Oracle **[BGP00]**
- NP $\subseteq$ BPP implies efficient algorithm
  - ¬OWF gives "*similar*" power on "*average*" **[IL89, OW93]**

Uniform Generation

- For NP relations **[JVV86]**:
  - Uniformly sample from $R^{-1}(x) = \{w \mid R(x; w) = 1\}$
  - Efficient algorithm using NP Oracle **[BGP00]**
- NP ⊆ BPP implies efficient algorithm
  - ¬OWF gives "*similar*" power on "*average*" **[IL89, OW93]**
- Used in computation of local randomness consistent with any partial transcript

Uniform Generation

Uniform Generation

Uniform Generation

Uniform Generation

Uniform Generation

Uniform Generation

Uniform Generation

Uniform Generation

Uniform Generation

Uniform Generation

- Sample Next bit

Uniform Generation

- Sample Next bit
- Sample Transcript extension

Uniform Generation

- Sample Next bit
- Sample Transcript extension
- Determine Color

General Attack [MPS10]

General Attack [MPS10]

- Need to attack at $\omega(1)$ rounds for more than $1/_{poly}$ bias

General Attack [MPS10]

- Need to attack at $\omega(1)$ rounds for more than $^1/_{poly}$ bias
- Greedy does not work

General Attack [MPS10]

- Need to attack at $\omega(1)$ rounds for more than $^1/_{poly}$ bias
- Greedy does not work
  - Greedy strategy for Alice and Bob

General Attack [MPS10]

- Need to attack at $\omega(1)$ rounds for more than $^1/_{poly}$ bias
- Greedy does not work
  - Greedy strategy for Alice and Bob
    - Malicious Alice outputs b such that $\chi_b \geq \chi$

General Attack [MPS10]

- Need to attack at $\omega(1)$ rounds for more than $^1/_{poly}$ bias
- Greedy does not work
  - Greedy strategy for Alice and Bob
    - Malicious Alice outputs b such that $\chi_b \geq \chi$
    - Malicious Bob outputs b such that $\chi_b \leq \chi$

General Attack [MPS10]

- Need to attack at $\omega(1)$ rounds for more than $^1/_{poly}$ bias
- Greedy does not work
  - Greedy strategy for Alice and Bob
    - Malicious Alice outputs b such that $\chi_b \geq \chi$
    - Malicious Bob outputs b such that $\chi_b \leq \chi$
  - There exists a protocol, where neither party can increase the probability of their preferred outcome beyond $^1/_2 + \nu$ using Greedy strategy, for negligible ν

General Attack [MPS10]

- Need to attack at $\omega(1)$ rounds for more than $^1/_{poly}$ bias
- Greedy does not work
  - Greedy strategy for Alice and Bob
    - Malicious Alice outputs b such that $\chi_b \geq \chi$
    - Malicious Bob outputs b such that $\chi_b \leq \chi$
  - There exists a protocol, where neither party can increase the probability of their preferred outcome beyond $^1/_2 + \nu$ using Greedy strategy, for negligible ν

General Attack [MPS10]

General Attack [MPS10]

- Hedged Greedy works

General Attack [MPS10]

- Hedged Greedy works
  - Probabilistic scheme instead of sharp threshold (Hedging the Bets)

General Attack [MPS10]

- Hedged Greedy works
  - Probabilistic scheme instead of sharp threshold (Hedging the Bets)
  - Intuition of Alice Strategy: Output b with probability proportional to $p_b\chi_b/(1-\chi_b)$

General Attack [MPS10]

- Hedged Greedy works
  - Probabilistic scheme instead of sharp threshold (Hedging the Bets)
  - Intuition of Alice Strategy: Output b with probability proportional to $p_b\chi_b/(1-\chi_b)$
- Remaining Problem: Estimating χ

General Attack [MPS10]

- Hedged Greedy works
  - Probabilistic scheme instead of sharp threshold (Hedging the Bets)
  - Intuition of Alice Strategy: Output b with probability proportional to $p_b\chi_b/(1-\chi_b)$
- Remaining Problem: Estimating χ
  - Reduce to "*stateless*" protocols

General Attack [MPS10]

- Hedged Greedy works
  - Probabilistic scheme instead of sharp threshold (Hedging the Bets)
  - Intuition of Alice Strategy: Output b with probability proportional to $p_b \chi_b / (1 - \chi_b)$
- Remaining Problem: Estimating χ
  - Reduce to "*stateless*" protocols
  - Handle Additive error in estimating χ

General Attack [MPS10]

- Hedged Greedy works
  - Probabilistic scheme instead of sharp threshold (Hedging the Bets)
  - Intuition of Alice Strategy: Output b with probability proportional to $p_b\chi_b/(1-\chi_b)$
- Remaining Problem: Estimating χ
  - Reduce to "*stateless*" protocols
  - Handle Additive error in estimating χ
- Tight for a class of algorithms

Analyzing the Attack

Analyzing the Attack

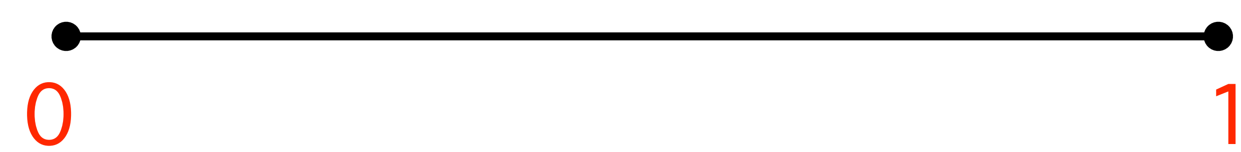
- A : Expectation of the outcome when Alice is malicious and Bob is honest

Analyzing the Attack

- A : Expectation of the outcome when Alice is malicious and Bob is honest
    - $F_A = (1-A) / (1-\chi)$: Failure of Alice's attack

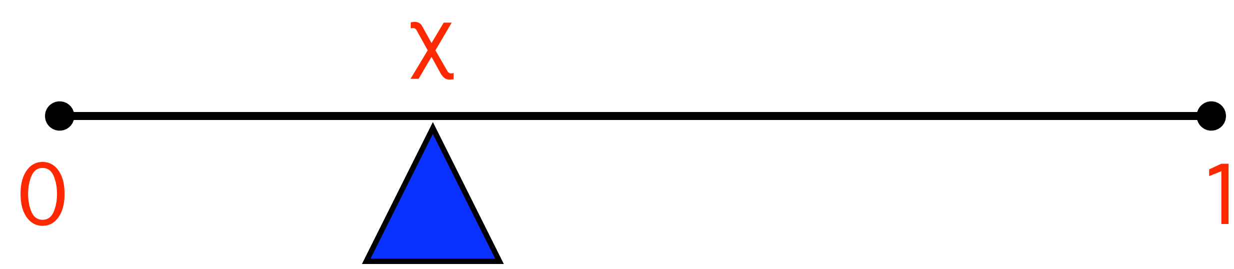
Analyzing the Attack

- A : Expectation of the outcome when Alice is malicious and Bob is honest
  - $F_A = (1-A) / (1-\chi)$: Failure of Alice's attack



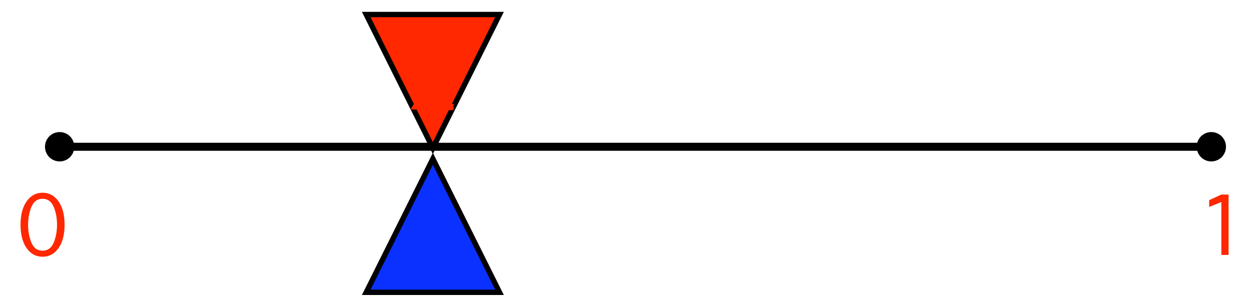
Analyzing the Attack

- A : Expectation of the outcome when Alice is malicious and Bob is honest
  - $F_A = (1-A) / (1-\chi)$: Failure of Alice's attack



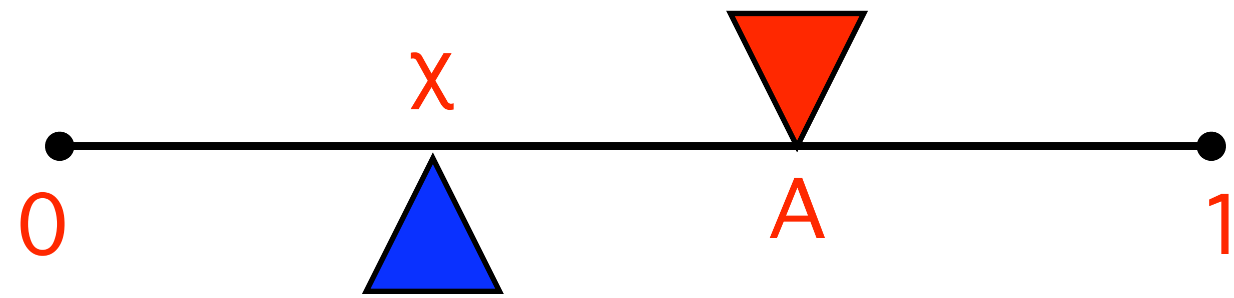
Analyzing the Attack

- A : Expectation of the outcome when Alice is malicious and Bob is honest
  - $F_A = (1-A) / (1-\chi)$: Failure of Alice's attack



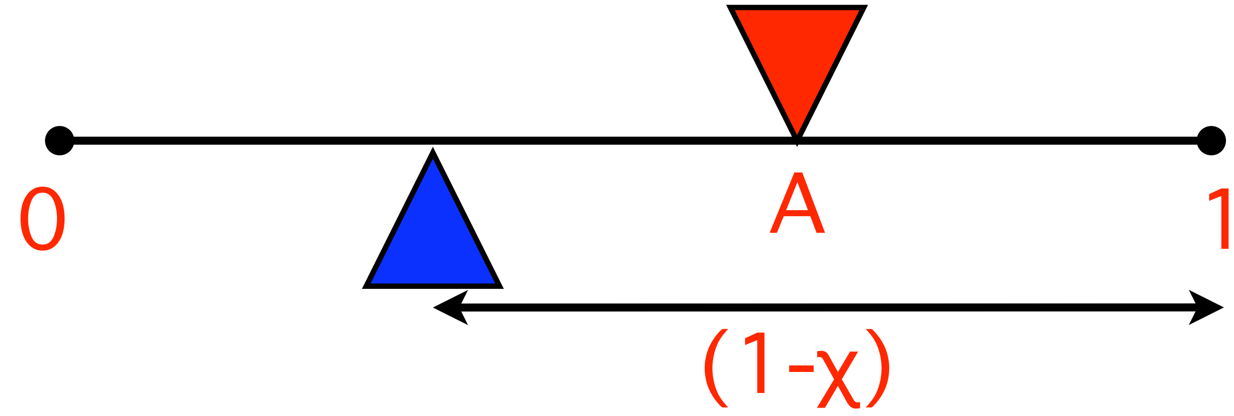
Analyzing the Attack

- A : Expectation of the outcome when Alice is malicious and Bob is honest
  - $F_A = (1-A) / (1-\chi)$: Failure of Alice's attack



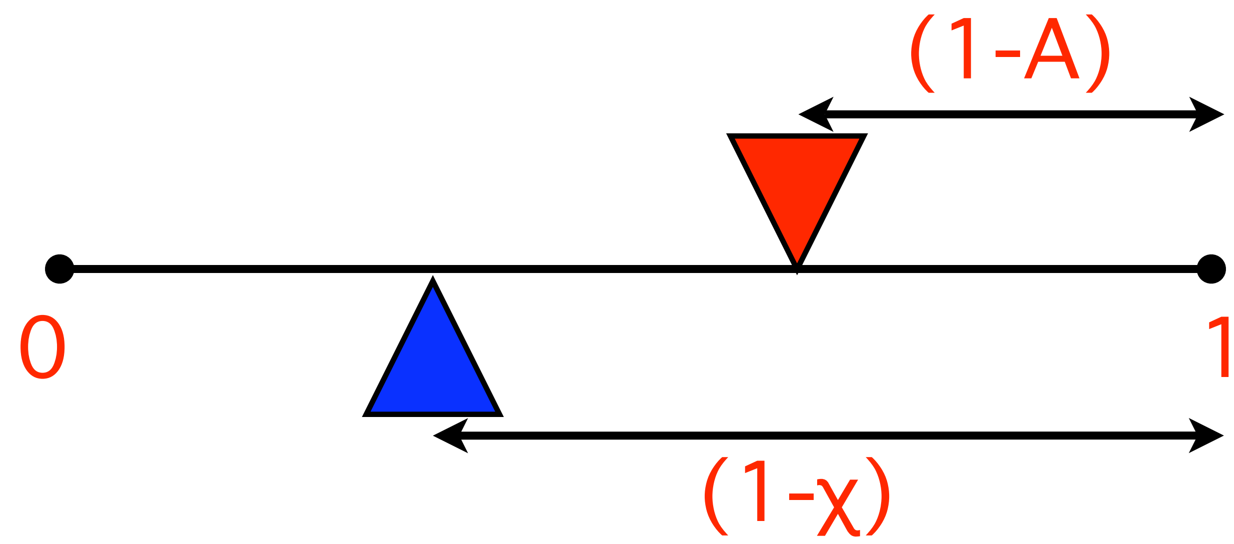
Analyzing the Attack

- A : Expectation of the outcome when Alice is malicious and Bob is honest
  - $F_A = (1-A) / (1-\chi)$: Failure of Alice's attack



Analyzing the Attack

- A : Expectation of the outcome when Alice is malicious and Bob is honest
  - $F_A = (1-A) / (1-\chi)$: Failure of Alice's attack



Analyzing the Attack

- A : Expectation of the outcome when Alice is malicious and Bob is honest
  - $F_A = (1-A) / (1-\chi)$: Failure of Alice's attack

Analyzing the Attack

- A : Expectation of the outcome when Alice is malicious and Bob is honest
  - $F_A = (1-A) / (1-\chi)$: Failure of Alice's attack
- B : Expectation of the outcome when Bob is malicious and Alice is honest

Analyzing the Attack

- A : Expectation of the outcome when Alice is malicious and Bob is honest
  - $F_A = (1-A) / (1-\chi)$: Failure of Alice's attack
- B : Expectation of the outcome when Bob is malicious and Alice is honest
  - $F_B = B / \chi$: Failure of Bob's attack

Analyzing the Attack

- A : Expectation of the outcome when Alice is malicious and Bob is honest
  - $F_A = (1-A) / (1-\chi)$: Failure of Alice's attack
- B : Expectation of the outcome when Bob is malicious and Alice is honest
  - $F_B = B / \chi$: Failure of Bob's attack

$$F_A + F_B \leq 1$$

Analyzing the Attack

- A : Expectation of the outcome when Alice is malicious and Bob is honest
    - $F_A = (1-A) / (1-\chi)$: Failure of Alice's attack
- B : Expectation of the outcome when Bob is malicious and Alice is honest
    - $F_B = B / \chi$: Failure of Bob's attack

$$F_A + F_B \leq 1$$

$$\min \{F_A , F_B\} \leq {}^1/_2$$

Analyzing the Attack

- A : Expectation of the outcome when Alice is malicious and Bob is honest
  - $F_A = (1-A) / (1-\chi)$: Failure of Alice's attack
- B : Expectation of the outcome when Bob is malicious and Alice is honest
  - $F_B = B / \chi$: Failure of Bob's attack

$$F_A + F_B \leq 1$$

$$\min \{F_A , F_B\} \leq {}^1/_2$$

Meta Theorem: Alice or Bob succeeds by half

$\chi = {}^1/_2$ means $A \geq {}^3/_4$ or $B \leq {}^1/_4$

Constant Alternation Attack [MPS10]

Constant Alternation Attack [MPS10]

- Sample a subtree of the Protocol Tree

Constant Alternation Attack [MPS10]

- Sample a subtree of the Protocol Tree
  - Every node has suitable poly degree

Constant Alternation Attack [MPS10]

- Sample a subtree of the Protocol Tree
  - Every node has suitable poly degree
  - Find the optimal message for the subtree by solving the corresponding "max-average" problem

Constant Alternation Attack [MPS10]

- Sample a subtree of the Protocol Tree
  - Every node has suitable poly degree
  - Find the optimal message for the subtree by solving the corresponding "max-average" problem
- Issues

Constant Alternation Attack [MPS10]

- Sample a subtree of the Protocol Tree
  - Every node has suitable poly degree
  - Find the optimal message for the subtree by solving the corresponding "max-average" problem
- Issues
  - Sampling a subtree can miss the max

Constant Alternation Attack [MPS10]

- Sample a subtree of the Protocol Tree
  - Every node has suitable poly degree
  - Find the optimal message for the subtree by solving the corresponding "max-average" problem
- Issues
  - Sampling a subtree can miss the max
  - As attack progresses, sampling gets "harder"

Constant Alternation Attack [MPS10]

- Sample a subtree of the Protocol Tree
  - Every node has suitable poly degree
  - Find the optimal message for the subtree by solving the corresponding "max-average" problem
- Issues
  - Sampling a subtree can miss the max
  - As attack progresses, sampling gets "harder"
    - But works for Constant Alternation protocols

Intuitive Summary

Intuitive Summary

+ OWF implies 1 secure Constant Alternation protocol **[Blum82, GL89, Naor89, HILL99]**

Intuitive Summary

+ OWF implies 1 secure Constant Alternation protocol [Blum82, GL89, Naor89, HILL99]

- General protocols

Intuitive Summary

+ OWF implies 1 secure Constant Alternation protocol [Blum82, GL89, Naor89, HILL99]

- General protocols

  - ε secure protocols imply PSPACE $\not\subseteq$ BPP

Intuitive Summary

+ OWF implies 1 secure Constant Alternation protocol **[Blum82, GL89, Naor89, HILL99]**

- General protocols
  - ε secure protocols imply PSPACE $\not\subseteq$ BPP
  - $1/2$ secure protocols imply NP $\not\subseteq$ BPP **[MPS10]**

Intuitive Summary

+ OWF implies 1 secure Constant Alternation protocol [Blum82, GL89, Naor89, HILL99]

- General protocols

  - ε secure protocols imply PSPACE $\not\subseteq$ BPP
  - $^1/_2$ secure protocols imply NP $\not\subseteq$ BPP [MPS10]
  - $1 - \theta(^1/_{\sqrt{k}})$ secure protocols implies OWF [CI93]

Intuitive Summary

\+ OWF implies 1 secure Constant Alternation protocol [Blum82, GL89, Naor89, HILL99]

\- General protocols

- ε secure protocols imply PSPACE $\not\subseteq$ BPP
- $1/2$ secure protocols imply NP $\not\subseteq$ BPP [MPS10]
- $1 - \theta(1/\sqrt{k})$ secure protocols implies OWF [CI93]

\- Constant Alternation protocols

Intuitive Summary

+ OWF implies 1 secure Constant Alternation protocol [Blum82, GL89, Naor89, HILL99]

- General protocols
  - ε secure protocols imply PSPACE $\not\subseteq$ BPP
  - $^1/_2$ secure protocols imply NP $\not\subseteq$ BPP [MPS10]
  - $1 - \theta(^1/_{\sqrt{k}})$ secure protocols implies OWF [CI93]

- Constant Alternation protocols
  - ε secure protocols imply OWF [MPS10]

Future Directions

Future Directions

- Does there exist a constant c such that, c secure General protocols imply OWF?

Future Directions

- Does there exist a constant c such that, c secure General protocols imply OWF?
  - Reworded: Does ¬OWF imply that some party can obtain his/her preferred outcome with probability at least $1 - c/2$?

Future Directions

- Does there exist a constant c such that, c secure General protocols imply OWF?
  - Reworded: Does ¬OWF imply that some party can obtain his/her preferred outcome with probability at least $1 - {}^{c}/_{2}$?
- Do ${}^{1}/_{poly}$ secure General protocols imply $NP \not\subseteq BPP$?

Future Directions

- Does there exist a constant c such that, c secure General protocols imply OWF?
  - Reworded: Does ¬OWF imply that some party can obtain his/her preferred outcome with probability at least $1 - {}^{c}/_{2}$?
- Do ${}^{1}/_{poly}$ secure General protocols imply $NP \not\subseteq BPP$?
  - Reworded: Does $NP \subseteq BPP$ imply that some party can obtain his/her preferred outcome with probability at least $1 - {}^{1}/_{poly}$?

Thank You