CS5322 Database Security

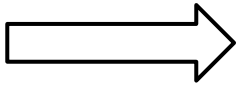
Last Lecture

- Three approaches for statistical databases
  - Query auditing
    - Query set size control
    - Query set overlap control
    - Linear systems for sum queries
    - Attacks based on query denial
  - Data perturbation
    - Generalization
    - Data swapping
    - Synthetic data generation
    - Random perturbation
  - Output perturbation

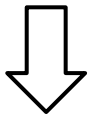
Data Swapping

- An approach used by the US Census Bureau to protect privacy in their census data release
- Idea: Swap some values among the tuples to make them non-identifying

Name	Age	Gender	Program	Grade
Alice	20	F	CS	70
Bob	21	M	CS	80
Cathy	22	F	IS	90
Daisy	23	M	IS	100



Age	Gender	Program	Grade
20	F	CS	70
21	M	CS	80
22	F	IS	90
23	M	IS	100

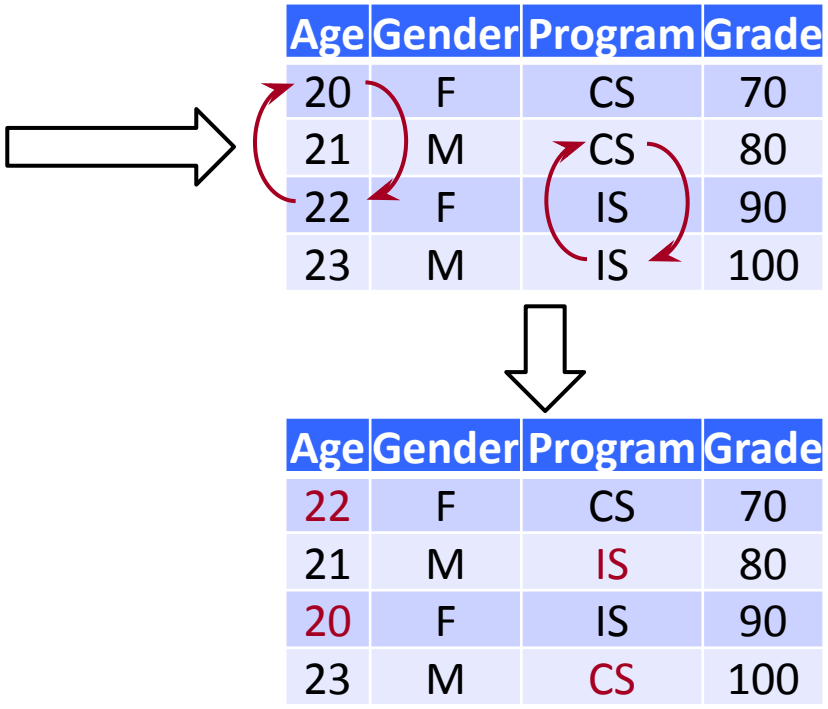


Age	Gender	Program	Grade
22	F	CS	70
21	M	IS	80
20	F	IS	90
23	M	CS	100

Data Swapping

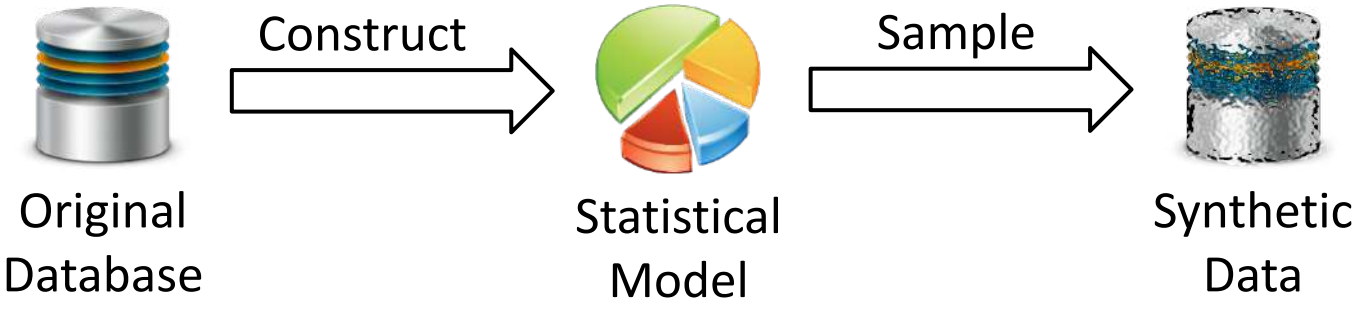
- Rationale:
  - After data swapping, the tuples are no longer “real”
  - This makes it difficult for an adversary to infer information
- Problem: There is no formal privacy guarantee

Name	Age	Gender	Program	Grade
Alice	20	F	CS	70
Bob	21	M	CS	80
Cathy	22	F	IS	90
Daisy	23	M	IS	100



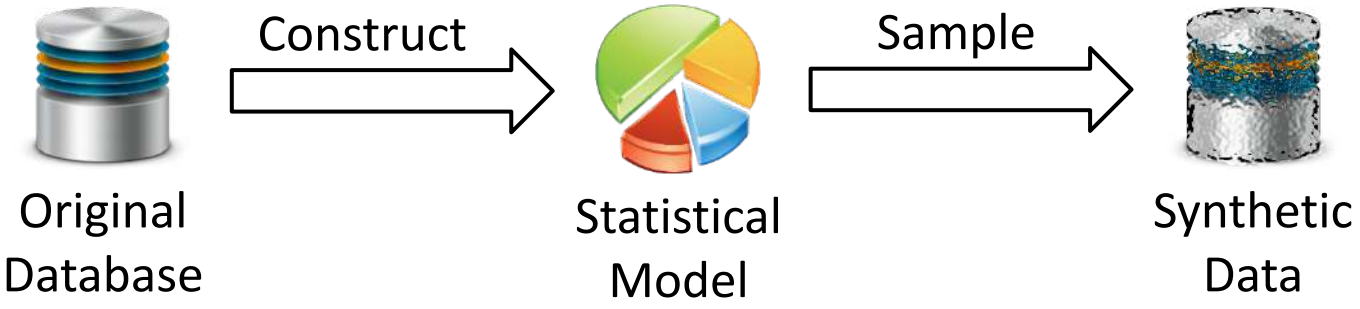
Synthetic Data Generation

- Another approach used by the US Census Bureau in some of their data release
- Idea:
  - Construct a statistical model of the original data
  - Generate synthetic data from the statistical model
- Rational:
  - All tuples are “synthetic”



Synthetic Data Generation

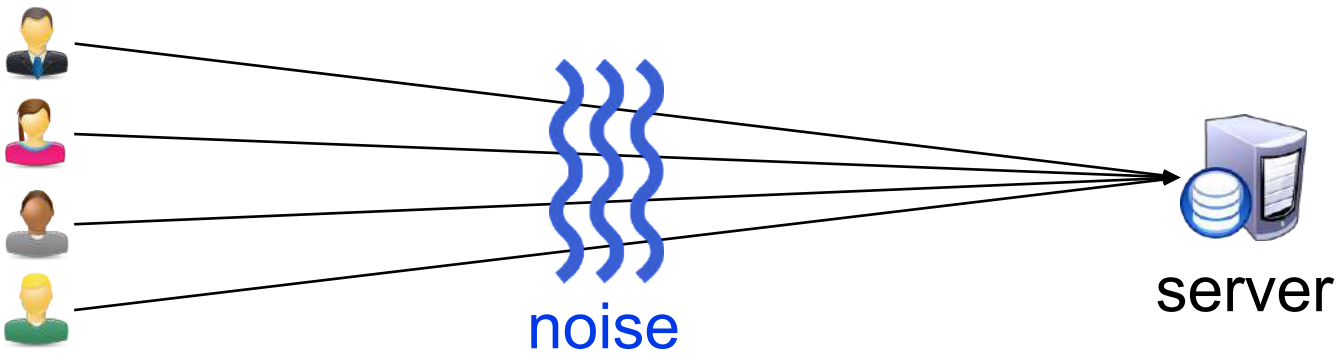
- Advantage over data swapping:
  - It is possible to provide some formal privacy guarantee
- How?
  - By injecting some noise into the statistical model
- We will not go into the details of this approach
  - Since the statistical models used are often complicated



Random Perturbation

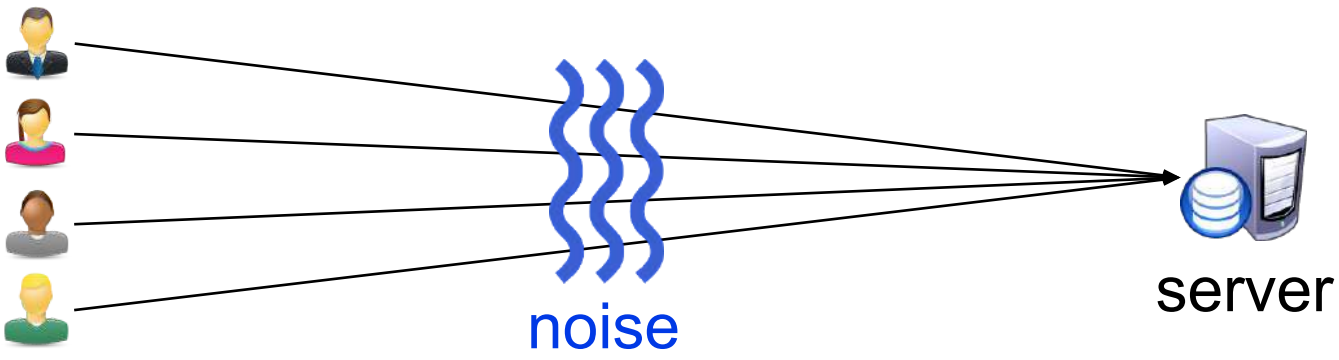
- This is an approach used by Google Chrome and Apple iOS to collect data from users
  - Google Chrome:
    - Which operating system is being used
    - What is the resolution of the monitor
    - …
  - Apple:
    - What new words you have typed
    - What emoji you have used
    - …

Random Perturbation: Setting



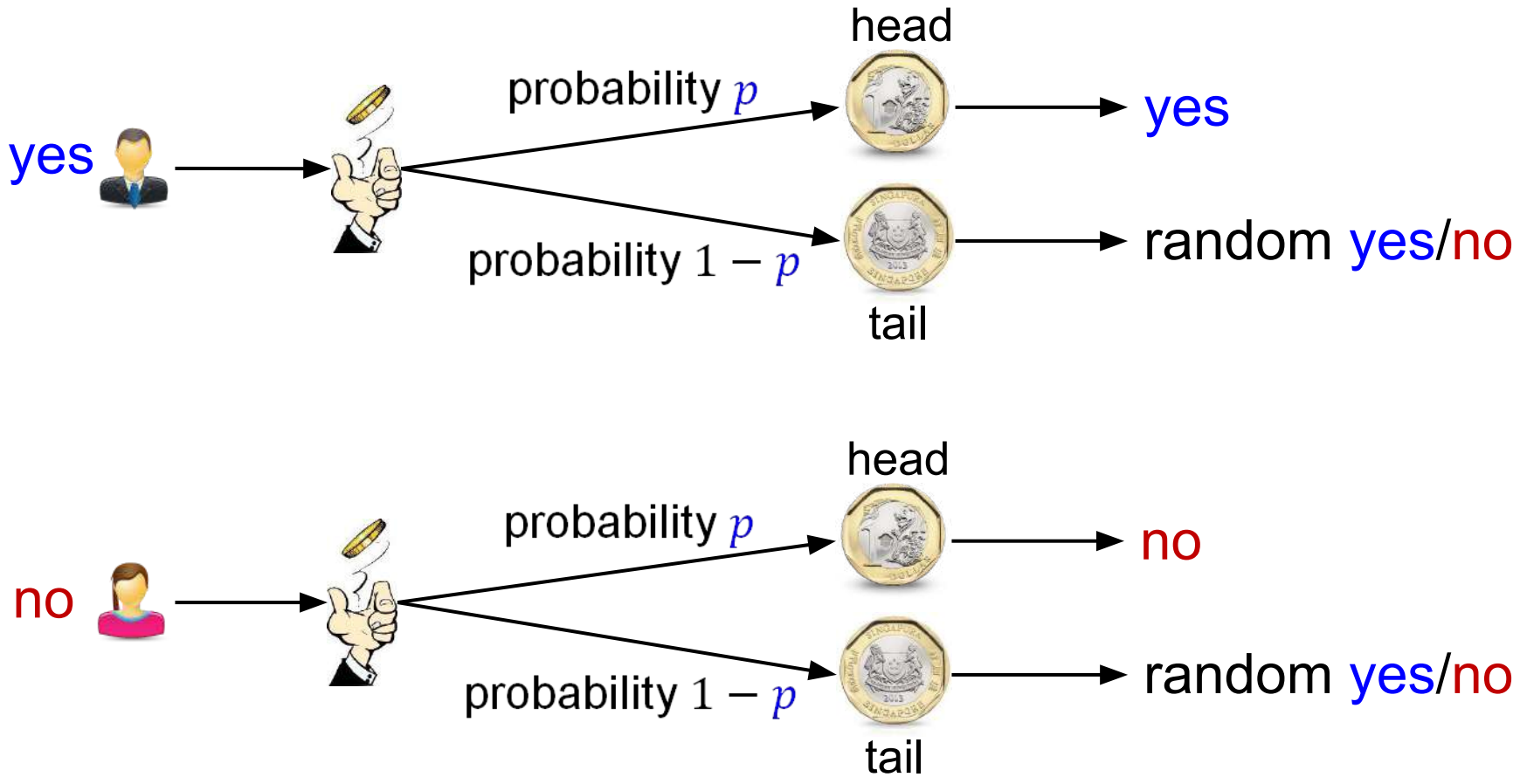
- Each user has a tuple
- They are asked to submit their tuples to a server
- For privacy protection, each user adds noise into her tuple before giving it to the server
- Objective:
  - Protect privacy, but allow the server to learn useful statistics

Random Perturbation: Setting

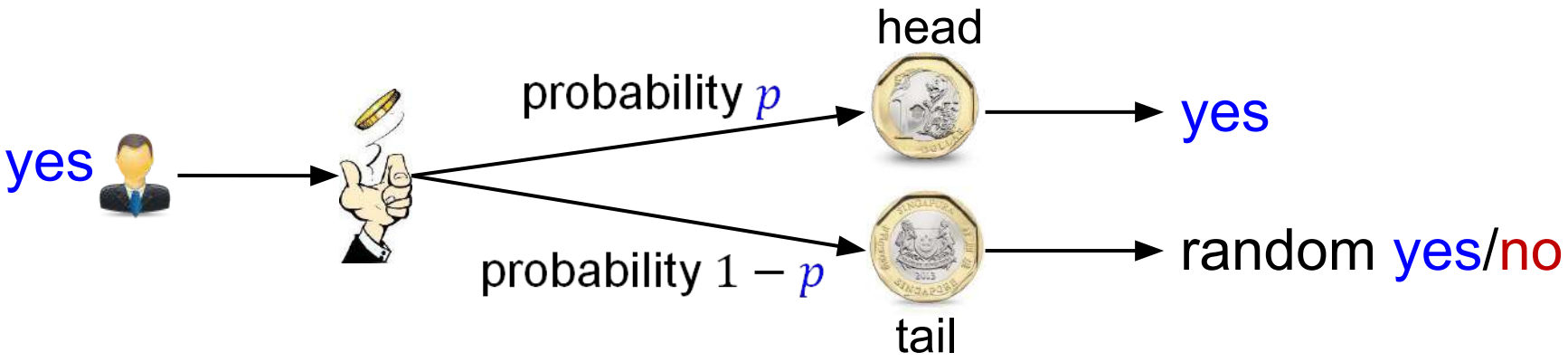


- Simplest setting:
  - The server asks each user: “Do you think Xiaokui is stupid?”
  - Each user has a yes-or-no answer
- Solution: Randomized Response [Warner 1965]
  - Each user gives her true answer with *p* probability
  - With the other 1 – *p* probability, she gives a random answer

Randomized response [Warner 1965]



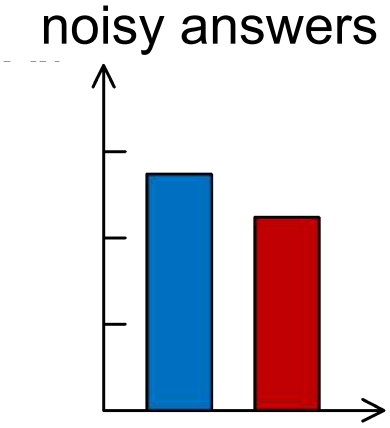
Randomized response [Warner 1965]



- Privacy: the respondent's real answer is not revealed
- Utility: the perturbed answers can still allow the server to estimate the survey results

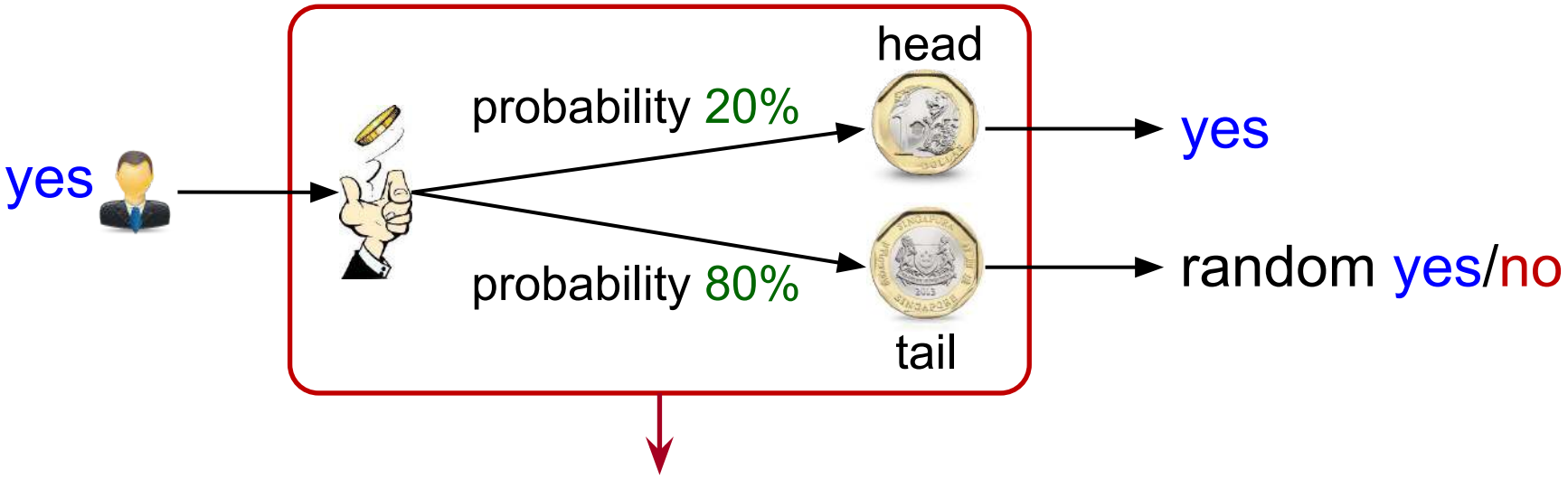
Getting Statistics from Noisy Answers

- Suppose that 10k people give me noisy answers
  - 5.5k yes, and 4.5k no
- I don't know exactly which answers are fake, but I know some statistics about the fake answers



Getting Statistics from Noisy Answers

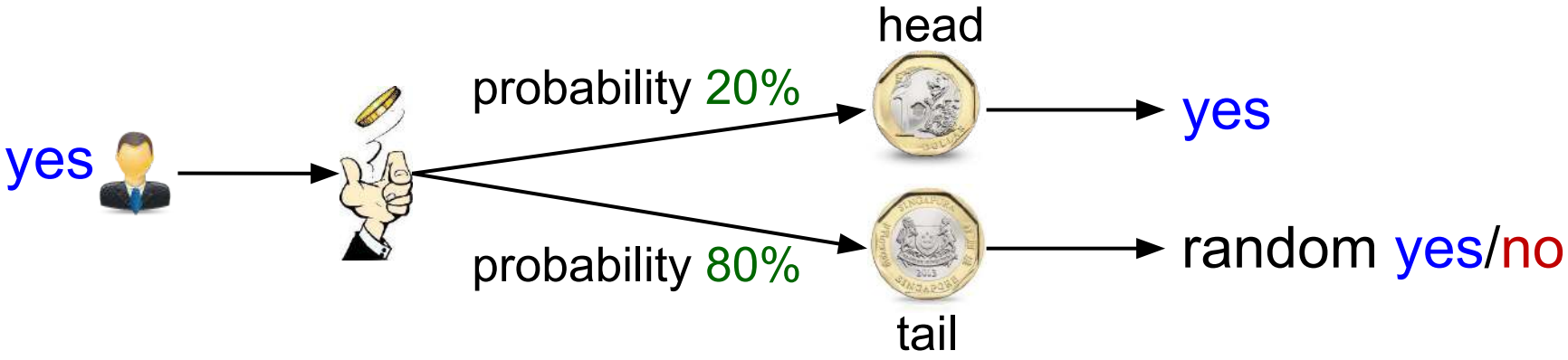
- Suppose that 10k people give me noisy answers
  - 5.5k yes, and 4.5k no
- I don't know exactly which answers are fake, but I know some statistics about the fake answers



I know that everyone gives a fake answer with 80% probability

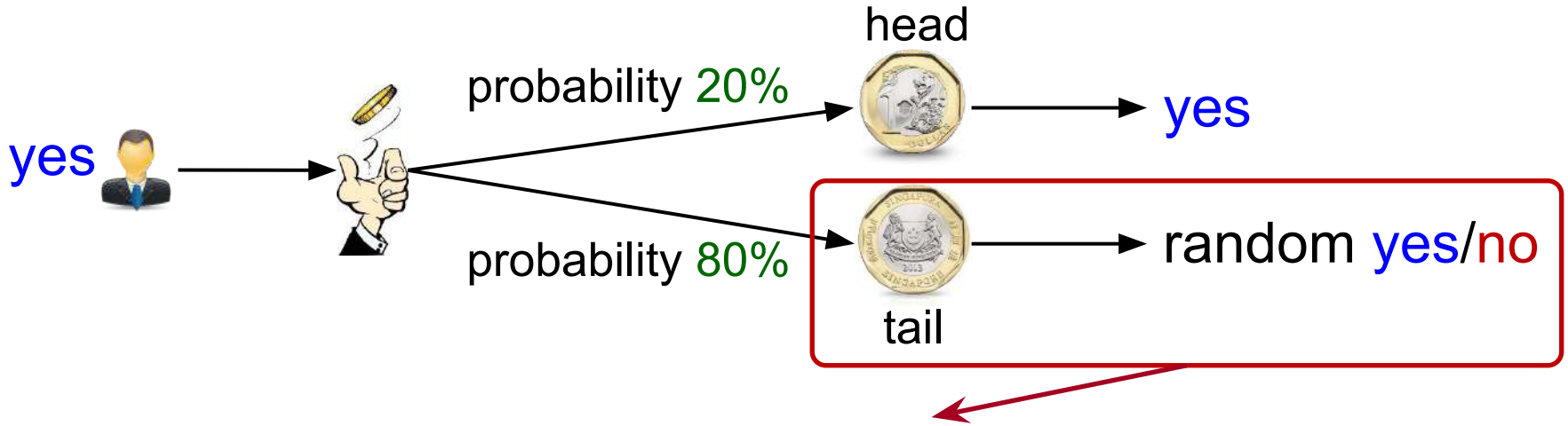
Getting Statistics from Noisy Answers

- Suppose that 10k people give me noisy answers
  - 5.5k yes, and 4.5k no
- Everyone gives a fake answer with 80% probability
  - So there are around 8k fake answers



Getting Statistics from Noisy Answers

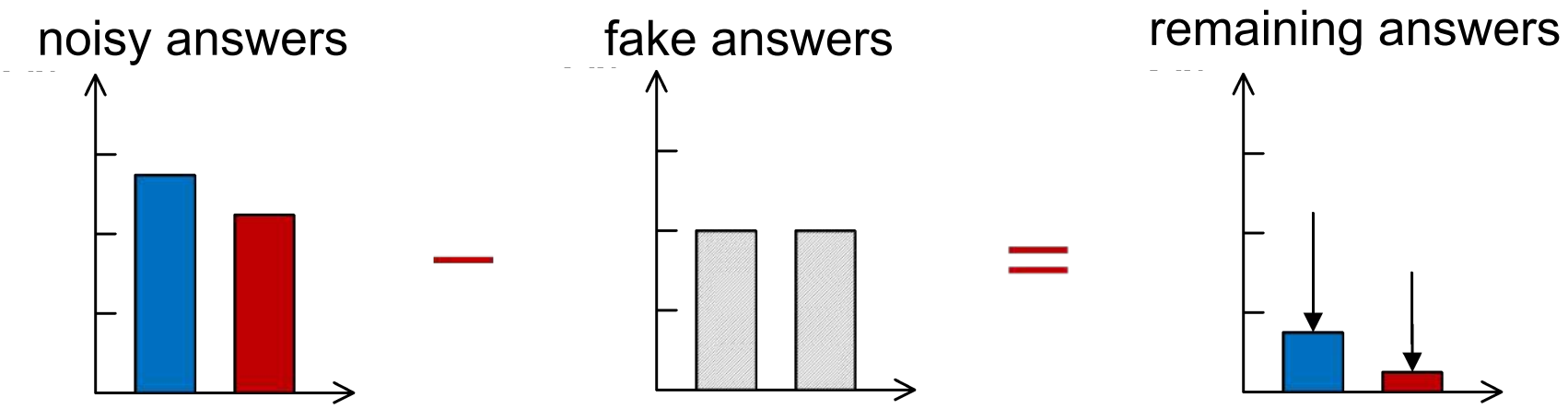
- Suppose that 10k people give me noisy answers
  - 5.5k yes, and 4.5k no
- Everyone gives a fake answer with 80% probability
  - So there are around 8k fake answers
  - Among them, roughly 4k yes and 4k no



I know that a fake answer has 50% probability to be yes, and 50% probability to be no

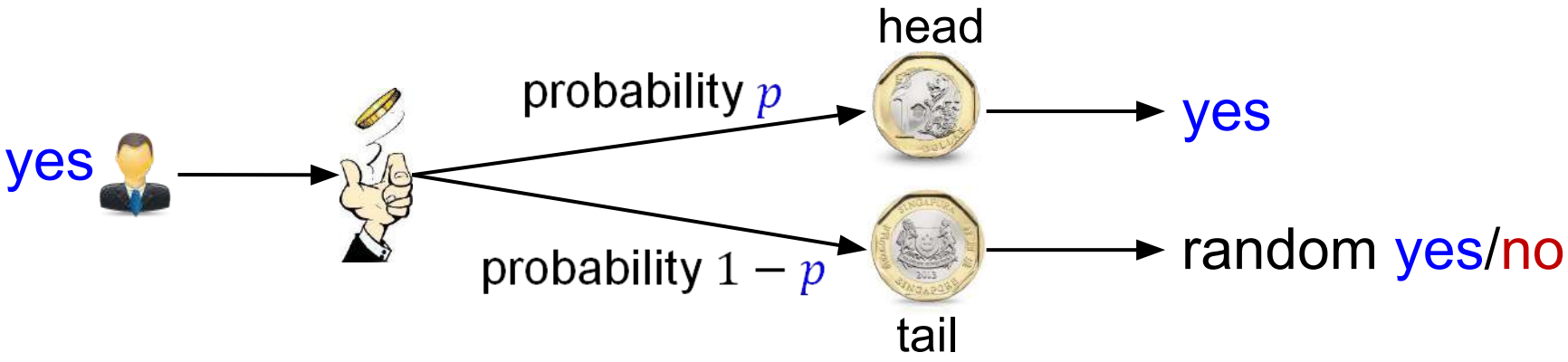
Getting Statistics from Noisy Answers

- Suppose that 10k people give me noisy answers
  - 5.5k yes, and 4.5k no
- Everyone gives a fake answer with 80% probability
  - So there are around 8k fake answers
  - Among them, roughly 4k yes and 4k no
- So the real answers are roughly 1.5k yes and 0.5k no
  - i.e., around 75% people's true answers are yes



Extension to More General Questions

- The previous example involves only a yes-or-no question
- But what if the question has more than two possible answers?
- Need to revise the algorithm for perturbation



Extension: Example

- Consider the following question: “Do you think that Xiaokui is stupid (S), very stupid (VS), or extremely stupid (ES)?”
- Suppose that your real answer is ES
- How should you perturb your answer?

ES 

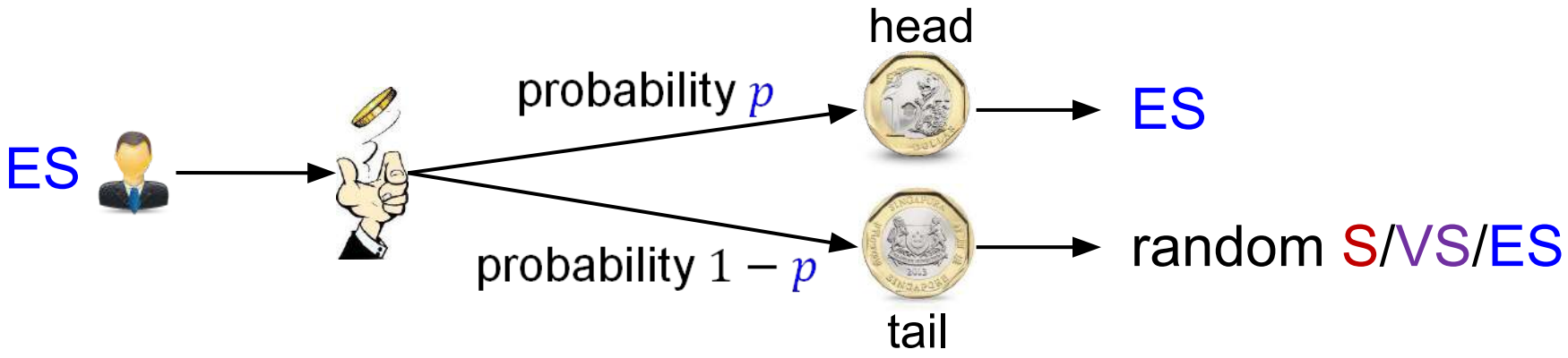
ES

VS

S

Extension: Example

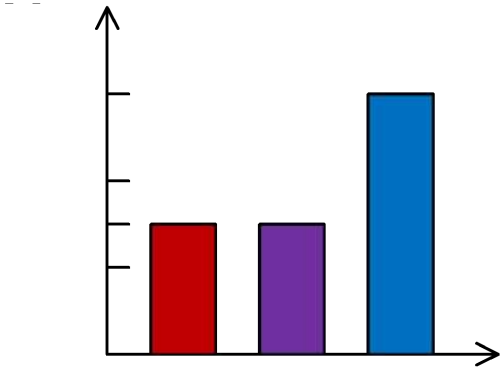
- Consider the following question: “Do you think that Xiaokui is stupid (S), very stupid (VS), or extremely stupid (ES)?”
- Suppose that your real answer is ES
- How should you perturb your answer?



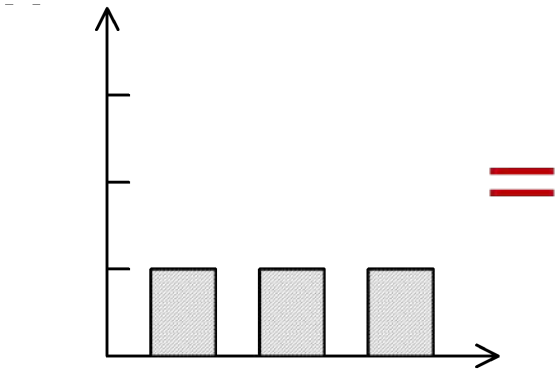
Extension: Example of Estimation

- 12k respondents; $p = 0.5$
  - i.e., with 50% probability, give random answers
- We know that around 6k respondents would give random answers
  - And those answers would be 1/3 S, 1/3 VS, and 1/3 ES

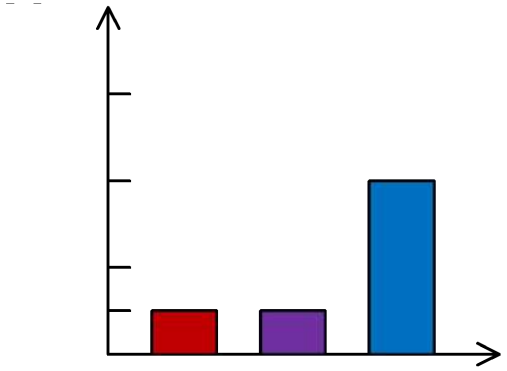
perturbed answers



estimated fake answers

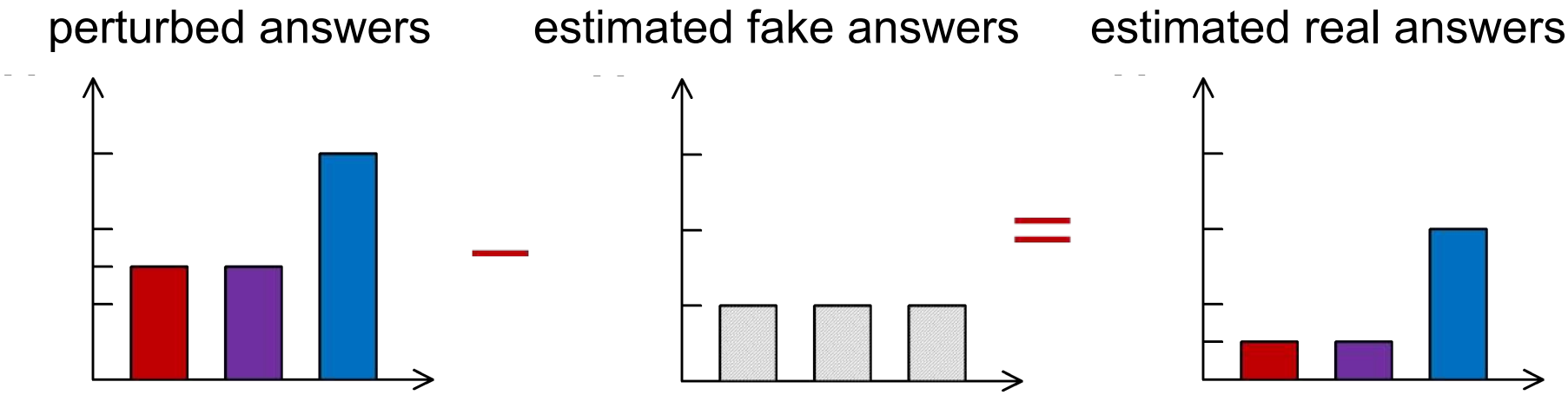


estimated real answers



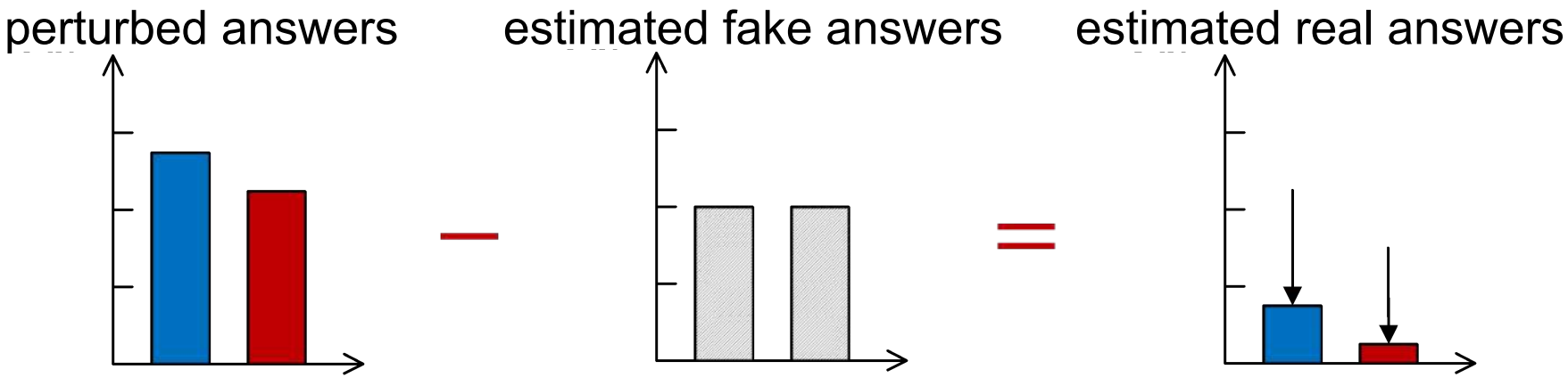
Extension: Example of Estimation

- Therefore, the real answers should be roughly 1/6 S, 1/6 VS, and 2/3 ES



Randomized Response: Rationale

- We know the distribution of noise introduced by randomized response
- So given the noisy distribution of data, we may infer the original distribution
- But we cannot infer much about any particular tuple
  - We can only learn high-level statistics
- So privacy is preserved



Extension to More General Questions

- The previous examples involve questions with a small number of possible answers
- What if the query's answer is numeric?
  - E.g., “What is your CS5322 grade?”
- Solution:
  - Let each user add some zero-mean random noise to their answers
- This allows the server to estimate the mean grade by taking the average of all noise answers
- Rationale:
  - The zero-mean noise tends to cancel each other out

Modern Extensions

- The previous examples showcase relatively simple perturbation techniques
- Practical applications often utilize more sophisticated perturbation methods
  - But they are built upon the simple techniques
- We will not go into the details

Randomized Response: Exercise

- Consider a revised version of randomized response for a yes-or-no survey
- Perturbation algorithm:
  - If the real answer is "no", then give 50% yes and 50% no
  - If the real answer is "yes“, then give 60% yes and 40% no
- Suppose that the noisy answers consist of 55% yes and 45% no
- Estimate the percentage of "yes" in the original answer

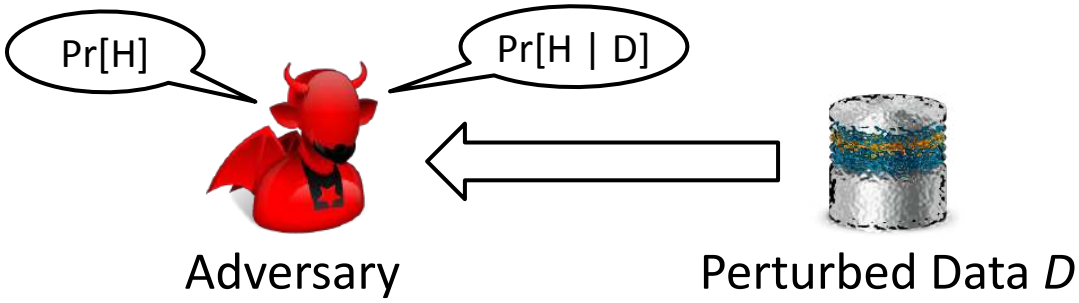
Coming Next

- Inference Analysis

Motivation

- Previously, we discussed a number of data perturbation techniques
  - Generalization, data swapping, synthetic data generation, randomized response
- We mentioned that it is important to evaluate the degree of protection provided by each method
- But how to do that in a rigorous way?
- We can utilize Bayesian inference

Bayesian Inference: General Idea



- The adversary has some *prior belief* Pr[H] about some hypotheses H
  - E.g., "Cedric has 75% chance to be stupid"
- After observing the perturbed data, the adversary has a *posterior belief* Pr[H | D]
  - E.g., "After observing Cedric's IQ test result, I believe that he has 99.9% chance to be stupid"
- We want the adversary to learn as little as possible
- So we measure the degree of protection provided by D by comparing Pr[H] with Pr[H | D]

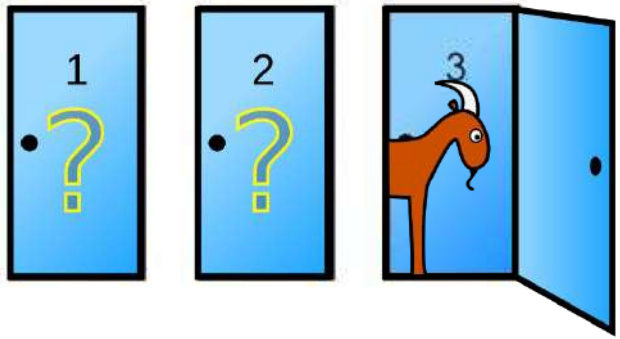
Bayesian Inference: Revisiting the Basics

- $\Pr[\, H \mid D \,] = \frac{\Pr[H \wedge D]}{\Pr[D]}$
- Example:
  - H: The final is difficult
  - D: The mid-term is difficult
  - Pr[H | D]: Given that the mid-term is difficult, what is the probability that the final is also difficult?
  - Pr[D]: We observe that in the previous semesters, there was 50% chance that the mid-term was difficult
  - Pr[H ∧ D]: We observe that in the previous semesters, there was 45% chance that the mid-term and final are both difficult
  - Pr[H | D] = Pr[H ∧ D] / Pr[D] = 90%
  - So given that the mid-term is difficult, there is 90% chance that the final is also difficult

Bayesian Inference: Revisiting the Basics

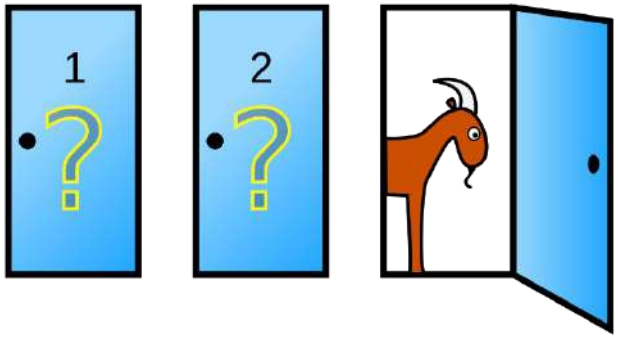
- $\Pr[H \mid D] = \frac{\Pr[H \wedge D]}{\Pr[D]} = \frac{\Pr[D|H] \cdot \Pr[H]}{\Pr[D]}$
- This is because Pr[H Λ D] = Pr[D | H] * Pr[H]
- Example:
  - The probability that both the final and mid-term are difficult equals
    - The probability that the final is difficult multiplied by
    - The conditional probability that, given a difficult final, the mid-term would also be difficult

Example: Monty Hall Problem



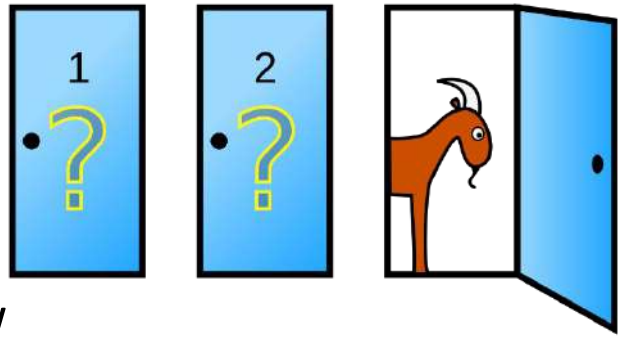
- Suppose you are on a game show, and you are given the choice of three doors
- Behind one door is a BMW; behind the others, goats.
- You pick a door, say No. 1
- The host, who knows what's behind the doors, opens another door, say No. 3, which has a goat.
- He then asks you, "Do you want to pick door No. 2?"
- Is it to your advantage to switch your choice?

Example: Monty Hall Problem



- You should switch
- Intuition:
  - Suppose that the host did not reveal what is behind Door 3
  - In that case, if we are to switch, we have two choices: Door 2 and Door 3
  - Choosing either one would lead to 1/3 winning probability
  - But now the host eliminates Door 3 for us
  - So when we switch, we have a higher probability to win

Example: Monty Hall Problem



- H: Door 2 has a BMW
- D: Host reveals Door 3 after you pick Door 1
- Pr[H] = 1/3
- Pr[H | D] = Pr[D | H] * Pr[H] / Pr[D]
  = Pr[D | H] * 1/3 / Pr[D]
- Pr[D | H] = 1
- Pr[D] = Pr[D ∧ H] + Pr[D ∧ (Door 1 has a BMW)] + Pr[D ∧ (Door 3 has a BMW)]
- = Pr[D | H] * Pr[H] + Pr[D | Door 1 has a BMW] * Pr[Door 1 has a BMW]
- = 1 * 1/3 + 1/2 * 1/3
- = 1/2
- So Pr[H | D] = 1 * 1/3 / (1/2) = 2/3
- In other words, it is beneficial to switch to Door 2

Inference Analysis: l-diversity

Name	Age	Gender	ZIP
Alice	20	F	100000
Bob	20	M	100000
Carl	50	M	190000
Dave	50	M	190000

What the adversary knows

Age	Gender	ZIP	Disease
20	*	100000	Flu
20	*	100000	Dyspepsia
50	*	190000	Gastritis
50	*	190000	Flu

Generalized Table *D*

- Suppose that the adversary knows the Age, Gender, and ZIP of everyone, and has the following prior belief:
  - Everyone has 1/3 chance to have flu, dyspepsia, and gastritis, respectively
  - The disease of everyone is independent
- What is the adversary's posterior belief that Alice has flu and Bob has dyspepsia?

Inference Analysis: l-diversity

Name	Age	Gender	ZIP
Alice	20	F	100000
Bob	20	M	100000
Carl	50	M	190000
Dave	50	M	190000

What the adversary knows

Age	Gender	ZIP	Disease
20	*	100000	Flu
20	*	100000	Dyspepsia
50	*	190000	Gastritis
50	*	190000	Flu

Generalized Table *D*

- H: Alice has flu and Bob has dyspepsia
- D: The first two tuples in the generalized table are as shown
- Pr[H]: 1/3 * 1/3 = 1/9
- $\Pr[H \mid D] = \frac{\Pr[D|H]\cdot\Pr[H]}{\Pr[D]} = \frac{\Pr[D|H]\cdot 1/9}{\Pr[D]}$
- Pr[D | H] = 100%, because when Alice has flu and Bob has dyspepsia, the first two tuples in the generalized table are always the same as what we observe
- $\Pr[H \mid D] = \frac{\Pr[D|H]\cdot\Pr[H]}{\Pr[D]} = \frac{\Pr[D|H]\cdot 1/9}{\Pr[D]} = \frac{1/9}{\Pr[D]}$

Inference Analysis: l-diversity

Name	Age	Gender	ZIP
Alice	20	F	100000
Bob	20	M	100000
Carl	50	M	190000
Dave	50	M	190000

What the adversary knows

Age	Gender	ZIP	Disease
20	*	100000	Flu
20	*	100000	Dyspepsia
50	*	190000	Gastritis
50	*	190000	Flu

Generalized Table *D*

- $\Pr[\, H \mid D \,] = \frac{1/9}{\Pr[D]}$
- Pr[D] = Pr[Alice has flu and Bob has dyspepsia]
  + Pr[Alice has dyspepsia and Bob has flu]
- = 1/9 + 1/9 = 2/9
- So Pr[H | D] = 1/2
- In other words, after observing D, the adversary has 50% confidence that Alice has flu and Bob has dyspepsia

Exercise

Name	Age	Gender	ZIP
Alice	20	F	100000
Bob	20	M	100000
Carl	50	M	190000
Dave	50	M	190000

What the adversary knows

Age	Gender	ZIP	Disease
20	*	100000	Flu
20	*	100000	Dyspepsia
50	*	190000	Gastritis
50	*	190000	Flu

Generalized Table *D*

- Suppose that the adversary knows the Age, Gender, and ZIP of every one, and has the following prior belief:
  - Alice has 1/2, 1/4, and 1/4 chances to have flu, dyspepsia, and gastritis, respectively
  - Bob has 1/3, 1/3, and 1/3 chances to have flu, dyspepsia, and gastritis, respectively
  - The disease of everyone is independent
- What is the adversary's posterior belief that Alice has flu and Bob has dyspepsia?

Exercise

Name	Age	Gender	ZIP
Alice	20	F	100000
Bob	20	M	100000
Carl	50	M	190000
Dave	50	M	190000

What the adversary knows

Age	Gender	ZIP	Disease
20	*	100000	Flu
20	*	100000	Dyspepsia
50	*	190000	Gastritis
50	*	190000	Flu

Generalized Table *D*

- H: Alice has flu and Bob has dyspepsia
- D: The first two tuples in the generalized table are as shown
- Pr[H]: 1/2 * 1/3 = 1/6
- $\Pr[H \mid D] = \frac{\Pr[D|H]\cdot\Pr[H]}{\Pr[D]} = \frac{\Pr[D|H]\cdot 1/6}{\Pr[D]}$
- Pr[D | H] = 100%, because when Alice has flu and Bob has dyspepsia, the first two tuples in the generalized table are always the same as what we observe
- $\Pr[H \mid D] = \frac{\Pr[D|H]\cdot\Pr[H]}{\Pr[D]} = \frac{\Pr[D|H]\cdot 1/6}{\Pr[D]} = \frac{1/6}{\Pr[D]}$

Exercise

Name	Age	Gender	ZIP
Alice	20	F	100000
Bob	20	M	100000
Carl	50	M	190000
Dave	50	M	190000

What the adversary knows

Age	Gender	ZIP	Disease
20	*	100000	Flu
20	*	100000	Dyspepsia
50	*	190000	Gastritis
50	*	190000	Flu

Generalized Table *D*

- $\Pr[\, H \mid D \,] = \frac{1/6}{\Pr[D]}$
- Pr[D] = Pr[Alice has flu and Bob has dyspepsia]
  + Pr[Alice has dyspepsia and Bob has flu]
- = 1/2*1/3 + 1/4*1/3 = 1/4
- So Pr[H | D] = 2/3
- In other words, after observing D, the adversary has 2/3 confidence that Alice has flu and Bob has dyspepsia

Exercise

Name	Age	Gender	ZIP
Alice	20	F	100000
Bob	20	M	100000
Carl	50	M	190000
Dave	50	M	190000

What the adversary knows

Age	Gender	ZIP	Disease
20	*	100000	Flu
20	*	100000	Dyspepsia
50	*	190000	Gastritis
50	*	190000	Flu

Generalized Table *D*

- Suppose that the adversary knows the Age, Gender, and ZIP of every one, and has the following prior belief:
  - Alice has p1, p2, and 1 – p1 – p2 probabilities to have flu, dyspepsia, and gastritis, respectively
  - Bob has p3, p4, and 1 – p3 – p4 probabilities to have flu, dyspepsia, and gastritis, respectively
  - The disease of everyone is independent
- What is the adversary's posterior belief that Alice has flu and Bob has dyspepsia?

Exercise

Name	Age	Gender	ZIP
Alice	20	F	100000
Bob	20	M	100000
Carl	50	M	190000
Dave	50	M	190000

What the adversary knows

Age	Gender	ZIP	Disease
20	*	100000	Flu
20	*	100000	Dyspepsia
50	*	190000	Gastritis
50	*	190000	Flu

Generalized Table *D*

- H: Alice has flu and Bob has dyspepsia
- D: The first two tuples in the generalized table are as shown
- Pr[H]: p1 * p4
- $\Pr[H \mid D] = \frac{\Pr[D|H]\cdot\Pr[H]}{\Pr[D]} = \frac{\Pr[D|H]\cdot p1\cdot p4}{\Pr[D]}$
- Pr[D | H] = 100%, because when Alice has flu and Bob has dyspepsia, the first two tuples in the generalized table are always the same as what we observe
- $\Pr[H \mid D] = \frac{\Pr[D|H]\cdot\Pr[H]}{\Pr[D]} = \frac{\Pr[D|H]\cdot p1\cdot p4}{\Pr[D]} = \frac{p1\cdot p4}{\Pr[D]}$

Exercise

Name	Age	Gender	ZIP
Alice	20	F	100000
Bob	20	M	100000
Carl	50	M	190000
Dave	50	M	190000

What the adversary knows

Age	Gender	ZIP	Disease
20	*	100000	Flu
20	*	100000	Dyspepsia
50	*	190000	Gastritis
50	*	190000	Flu

Generalized Table *D*

- $\Pr[\, H \mid D \,] = \frac{p1 \cdot p4}{\Pr[D]}$
- Pr[D] = Pr[Alice has flu and Bob has dyspepsia]
  + Pr[Alice has dyspepsia and Bob has flu]
- = p1*p4 + p2*p3
- So $\Pr[\, H \mid D \,] = \frac{p1 \cdot p4}{p1 \cdot p4 + p2 \cdot p3}$
- The adversary's belief changes from $p1 \cdot p4$ to $\frac{p1 \cdot p4}{p1 \cdot p4 + p2 \cdot p3}$ after observing D

there is no worse case
garuntee in terms of chnage

Exercise

Name	Age	Gender	ZIP
Alice	20	F	100000
Bob	20	M	100000
Carl	50	M	190000
Dave	50	M	190000

What the adversary knows

Age	Gender	ZIP	Disease
20	*	100000	Flu
20	*	100000	Dyspepsia
50	*	190000	Gastritis
50	*	190000	Flu

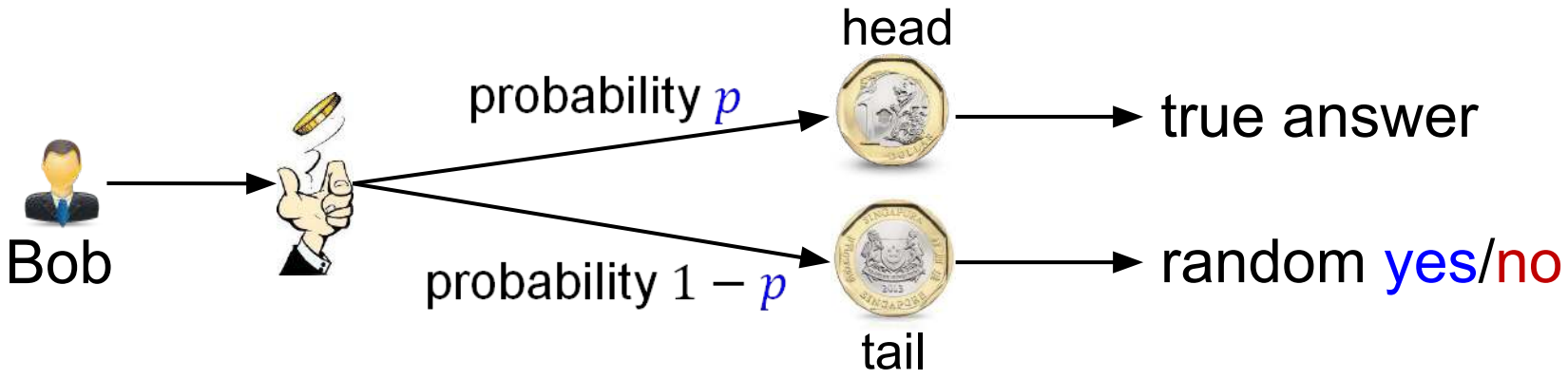
Generalized Table *D*

- The adversary's belief changes from $p1 \cdot p4$ to $\frac{p1 \cdot p4}{p1 \cdot p4 + p2 \cdot p3}$ after observing D
- How different can $p1 \cdot p4$ and $\frac{p1 \cdot p4}{p1 \cdot p4 + p2 \cdot p3}$ be?
- The difference can be arbitrarily large
  - Unless we make some assumptions about p1, p2, p3, p4
- This explains why we need to take into account the adversary's background knowledge when applying l-diversity

Coming Next

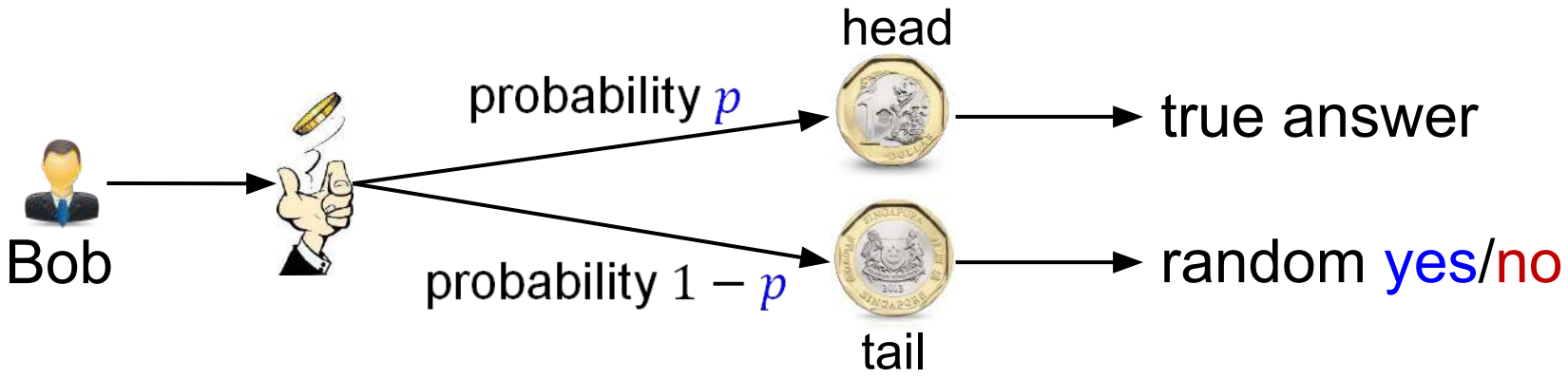
- Inference analysis for randomized response

Inference Analysis: Randomized Response



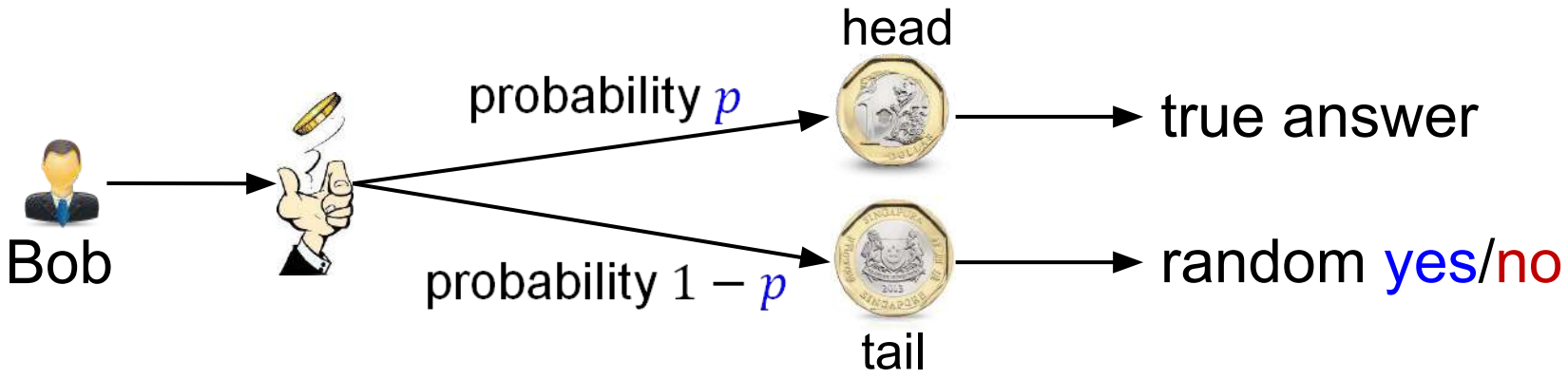
- Suppose that the adversary has the following prior belief:
  - Bob's true answer is yes with 60%, and no with 40% probability
- Assume that
  - The retention probability p = 1/5
  - Bob's perturbed answer is yes
- What is the adversary's posterior belief that Bob's true answer is yes?

Inference Analysis: Randomized Response



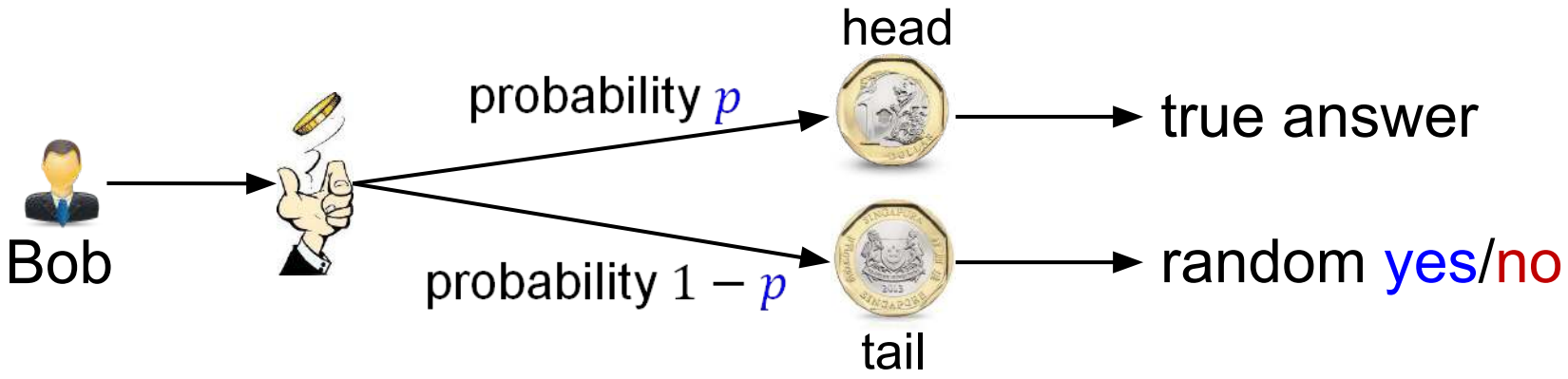
- H: Bob's true answer is yes
- D: Bob's perturbed answer is yes
- Pr[H] = 60%
- $\Pr[\,H \mid D\,] = \frac{\Pr[D|H]\cdot\Pr[H]}{\Pr[D]} = \frac{\Pr[D|H]\cdot 60\%}{\Pr[D]}$
- Pr[D | H] = 1/5 + 4/5 * 1/2 = 3/5
- $\Pr[\,H \mid D\,] = \frac{\Pr[D|H]\cdot\Pr[H]}{\Pr[D]} = \frac{\Pr[D|H]\cdot 60\%}{\Pr[D]} = \frac{9/25}{\Pr[D]}$

Inference Analysis: Randomized Response



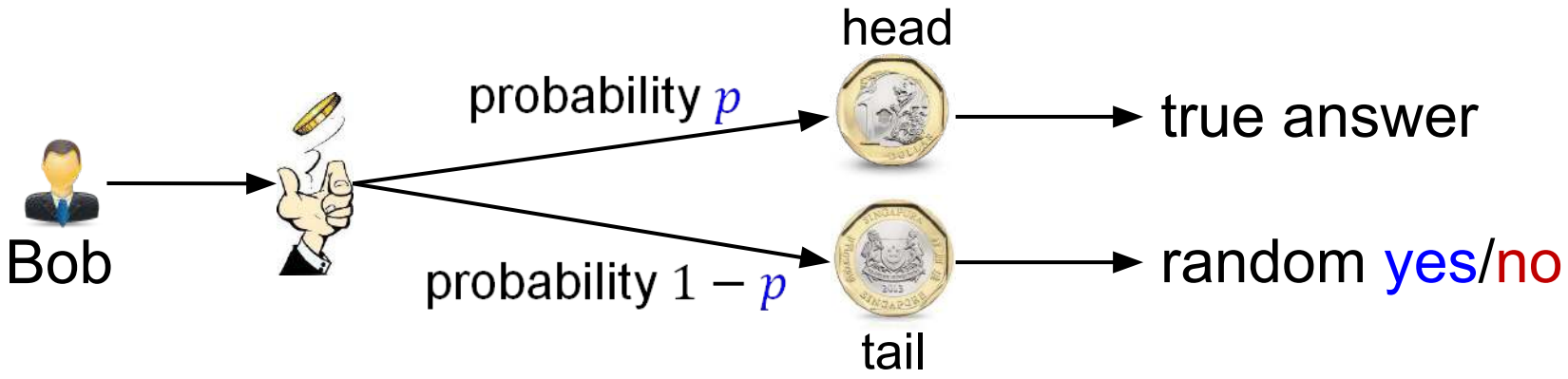
- H: Bob's true answer is yes
- D: Bob's perturbed answer is yes
- Pr[H] = 60%
- $\Pr[H \mid D] = \frac{\Pr[D|H]\cdot\Pr[H]}{\Pr[D]} = \frac{\Pr[D|H]\cdot 60\%}{\Pr[D]} = \frac{9/25}{\Pr[D]}$
- Pr[D] = Pr[D ∧ H] + Pr[D ∧ (not H)]
  = Pr[D | H] * Pr [H] + Pr[D | not H] * Pr[not H]
  = 9/25 + (4/5 * 1/2) * 40% = 13/25
- $\Pr[H \mid D] = \frac{\Pr[D|H]\cdot\Pr[H]}{\Pr[D]} = \frac{\Pr[D|H]\cdot 60\%}{\Pr[D]} = \frac{9/25}{\Pr[D]} = \frac{9}{13}$

Inference Analysis: Randomized Response



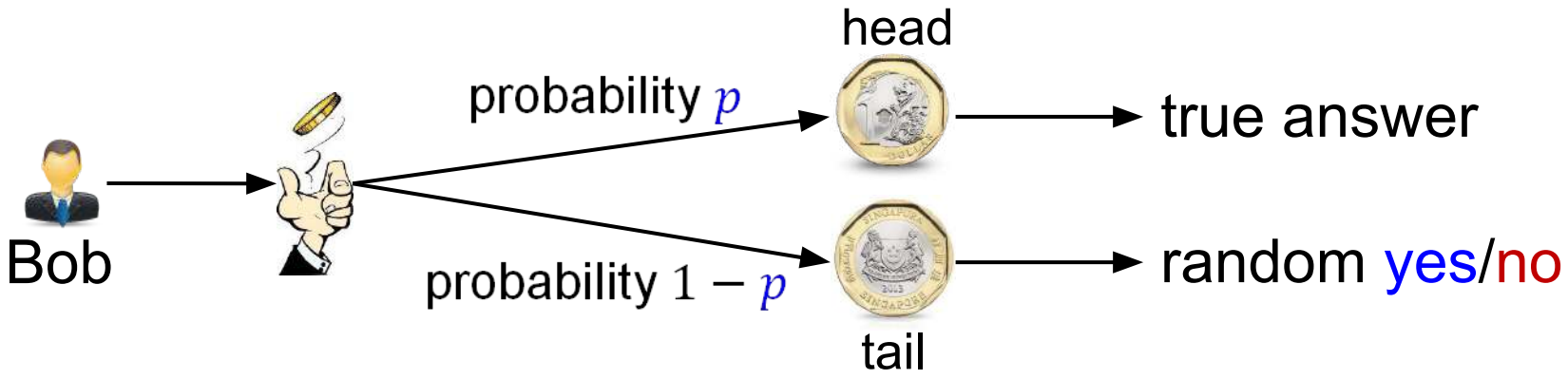
- H: Bob's true answer is yes
- D: Bob's perturbed answer is yes
- Pr[H] = 60%
- $\Pr[\,H \mid D\,] = \frac{\Pr[D|H]\cdot\Pr[H]}{\Pr[D]} = \frac{\Pr[D|H]\cdot 3/5}{\Pr[D]} = \frac{9/25}{\Pr[D]} = \frac{9}{13}$
- In other words, the adversary's belief changes from 60% to 9/13
  - this is an increase of around 15% only

Exercise



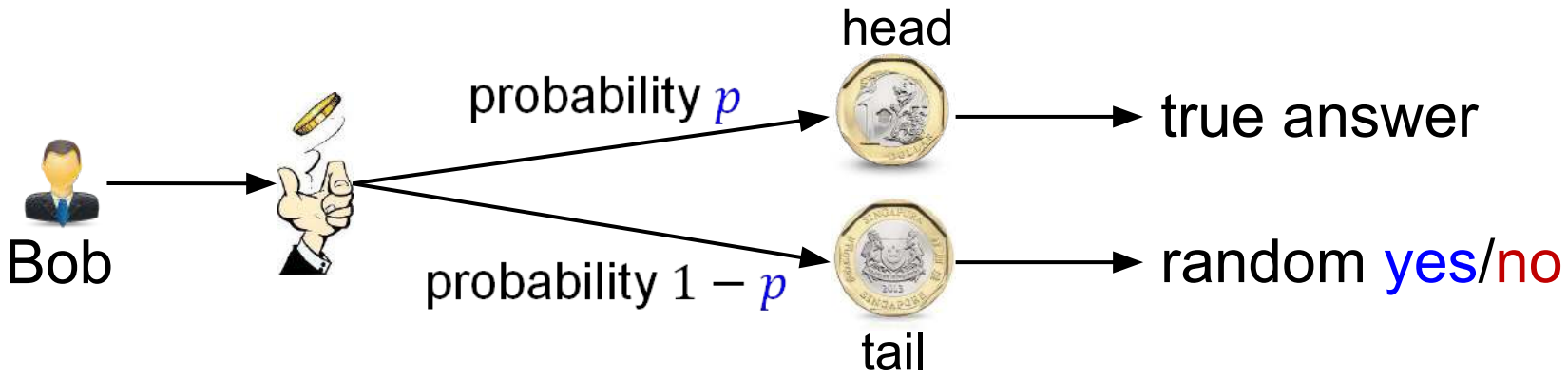
- Suppose that the adversary has the following prior belief:
  - Bob has 75% probability to answer yes, and 25% probability to answer no
- Assume that
  - The retention probability p = 1/4
  - Bob's perturbed answer is no
- What is the adversary's posterior belief that Bob's true answer is yes?

Exercise



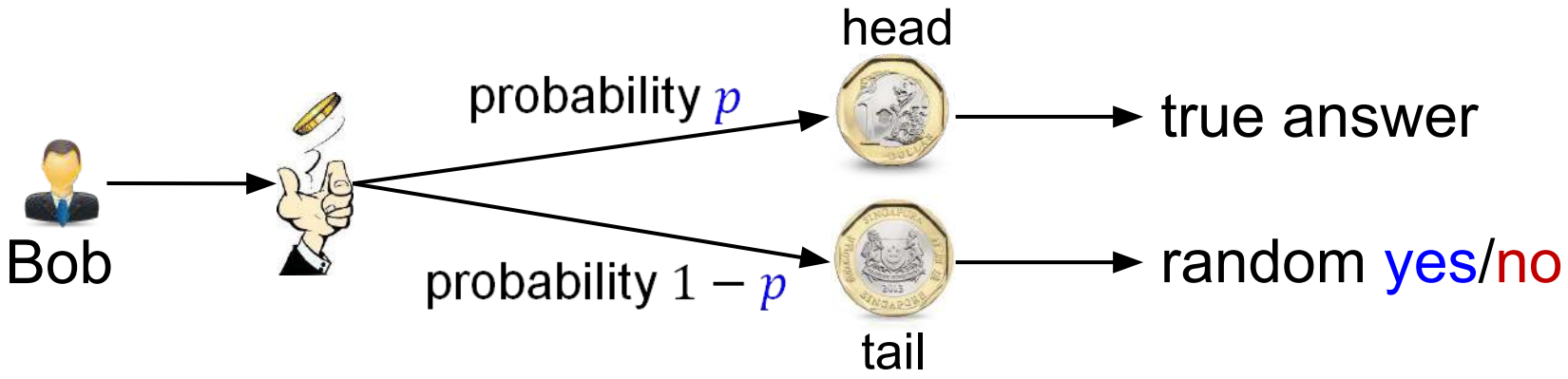
- H: Bob's true answer is yes
- D: Bob's perturbed answer is no
- Pr[H] = 75%
- $\Pr[H \mid D] = \frac{\Pr[D|H]\cdot\Pr[H]}{\Pr[D]} = \frac{\Pr[D|H]\cdot 75\%}{\Pr[D]}$
- Pr[D | H] = 3/4 * 1/2 = 3/8
- $\Pr[H \mid D] = \frac{\Pr[D|H]\cdot\Pr[H]}{\Pr[D]} = \frac{\Pr[D|H]\cdot 75\%}{\Pr[D]} = \frac{9/32}{\Pr[D]}$

Exercise



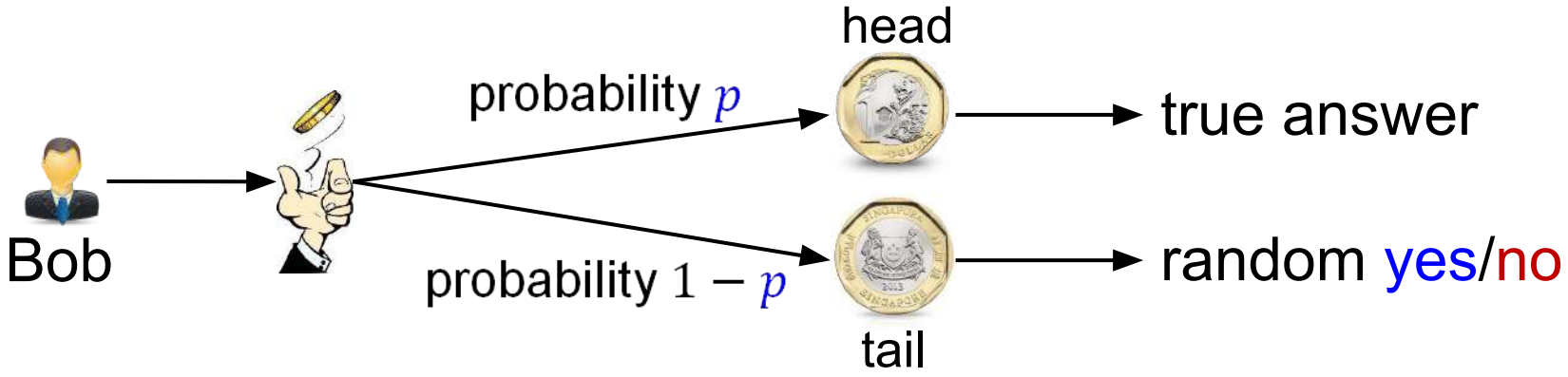
- H: Bob's true answer is yes
- D: Bob's perturbed answer is no
- Pr[H] = 75%
- $\Pr[H \mid D] = \frac{\Pr[D|H]\cdot\Pr[H]}{\Pr[D]} = \frac{\Pr[D|H]\cdot 75\%}{\Pr[D]} = \frac{9/32}{\Pr[D]}$
- Pr[D] = Pr[D ^ H] + Pr[D ^ (not H)]
  = Pr[D | H] * Pr [H] + Pr[D | not H] * Pr[not H]
  = 9/32 + (1/4 + 3/4 * 1/2) * 25% = 14/32
- $\Pr[H \mid D] = \frac{\Pr[D|H]\cdot\Pr[H]}{\Pr[D]} = \frac{\Pr[D|H]\cdot 3/5}{\Pr[D]} = \frac{9/32}{\Pr[D]} = \frac{9}{14}$

Exercise



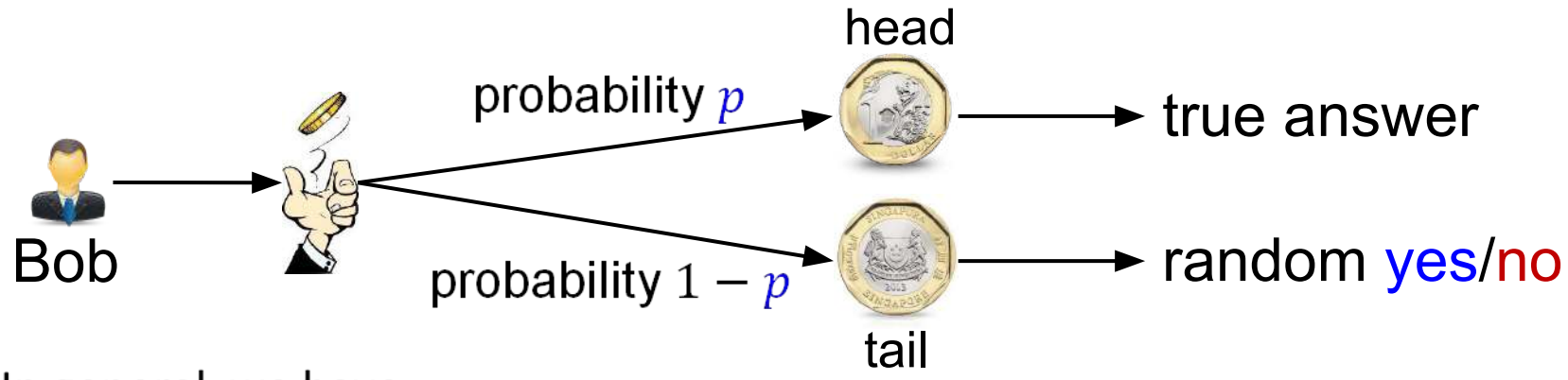
- H: Bob's true answer is yes
- D: Bob's perturbed answer is no
- Pr[H] = 75%
- $\Pr[\,H \mid D\,] = \frac{\Pr[D|H]\cdot\Pr[H]}{\Pr[D]} = \frac{\Pr[D|H]\cdot 3/5}{\Pr[D]} = \frac{9/32}{\Pr[D]} = \frac{9}{14}$
- In other words, the adversary's belief changes from 75% to 9/14
  - this is a decrease of around 14% only

The General Case



- Assume that the retention probability is p
- H: The adversary's prior belief on Bob's answer
- D: Bob's perturbed answer
- How large and small can $\frac{\Pr[H|D]}{\Pr[H]}$ be?

Inference Analysis: Randomized Response



- In general, we have
- $$\frac{\Pr[H|D]}{\Pr[H]} = \frac{\Pr[D|H]\cdot\Pr[H]/\Pr[D]}{\Pr[H]} = \frac{\Pr[D|H]}{\Pr[D]} = \frac{\Pr[D|H]}{\Pr[D\wedge H]+\Pr[D\wedge(not\ H)]}$$
- $$= \frac{\Pr[D|H]}{\Pr[D|H]\cdot\Pr[H]+\Pr[D|(not\ H)]\cdot\Pr[not\ H]} = \frac{\Pr[D|H]}{\Pr[D|H]\cdot\Pr[H]+\Pr[D|(not\ H)]\cdot(1-\Pr[H])}$$

- There are only two possibilities for $\Pr[D \mid H]$ and $\Pr[D \mid (not\ H)]$:
  - $\Pr[D \mid H] = p + \frac{1-p}{2}$ and $\Pr[D \mid (not\ H)] = \frac{1-p}{2}$, or
  - $\Pr[D \mid H] = \frac{1-p}{2}$ and $\Pr[D \mid (not\ H)] = p + \frac{1-p}{2}$

Inference Analysis: Randomized Response

- In general, we have
- $$\frac{\Pr[H|D]}{\Pr[H]} = \frac{\Pr[D|H]\cdot\Pr[H]/\Pr[D]}{\Pr[H]} = \frac{\Pr[D|H]}{\Pr[D]} = \frac{\Pr[D|H]}{\Pr[D\wedge H]+\Pr[D\wedge(not\ H)]}$$
- $$= \frac{\Pr[D|H]}{\Pr[D|H]\cdot\Pr[H]+\Pr[D|(not\ H)]\cdot\Pr[not\ H]} = \frac{\Pr[D|H]}{\Pr[D|H]\cdot\Pr[H]+\Pr[D|(not\ H)]\cdot(1-\Pr[H])}$$

- There are only two possibilities for $\Pr[D \mid H]$ and $\Pr[D \mid (not\ H)]$:
  - $\Pr[D \mid H] = p + \frac{1-p}{2}$ and $\Pr[D \mid (not\ H)] = \frac{1-p}{2}$, or
  - $\Pr[D \mid H] = \frac{1-p}{2}$ and $\Pr[D \mid (not\ H)] = p + \frac{1-p}{2}$

- Accordingly, $\frac{\Pr[H|D]}{\Pr[H]}$ only has two possibilities:
  - $$\frac{\Pr[H|D]}{\Pr[H]} = \frac{p+\frac{1-p}{2}}{\left(p+\frac{1-p}{2}\right)\cdot\Pr[H]+\frac{1-p}{2}\cdot(1-\Pr[H])} = \frac{1+p}{1-p+2p\cdot\Pr[H]} \leq \frac{1+p}{1-p}$$
  - $$\frac{\Pr[H|D]}{\Pr[H]} = \frac{\frac{1-p}{2}}{\left(\frac{1-p}{2}\right)\cdot\Pr[H]+\left(p+\frac{1-p}{2}\right)\cdot(1-\Pr[H])} = \frac{1-p}{1+p-2p\cdot\Pr[H]} \geq \frac{1-p}{1+p}$$

Inference Analysis: Randomized Response

- Conclusion: $\frac{1-p}{1+p} \leq \frac{\Pr[H|D]}{\Pr[H]} \leq \frac{1+p}{1-p}$
- In other words, randomized response only change the adversary's belief by a factor of $\frac{1+p}{1-p}$
  - Regardless of what the adversary's prior belief is
- This is a much stronger guarantee than what l-diversity offers