Quantifying Information Leakage of Deterministic Encryption

Mireya Jurado and Geoffrey Smith

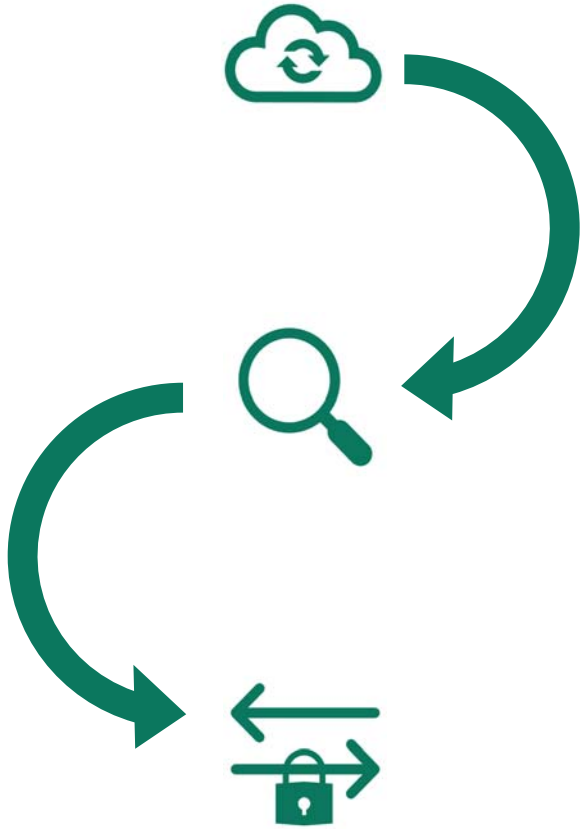
November 11, 2019

CCSW 2019: Cloud Computing Security Workshop

FIU
Engineering & Computing
School of Computing & Information Sciences

Challenge

- We want to store sensitive data remotely
- Encrypted databases aim to balance security and functionality



Question: How do you measure information leakage of deterministic encryption?

Quantitative Information Flow (QIF)

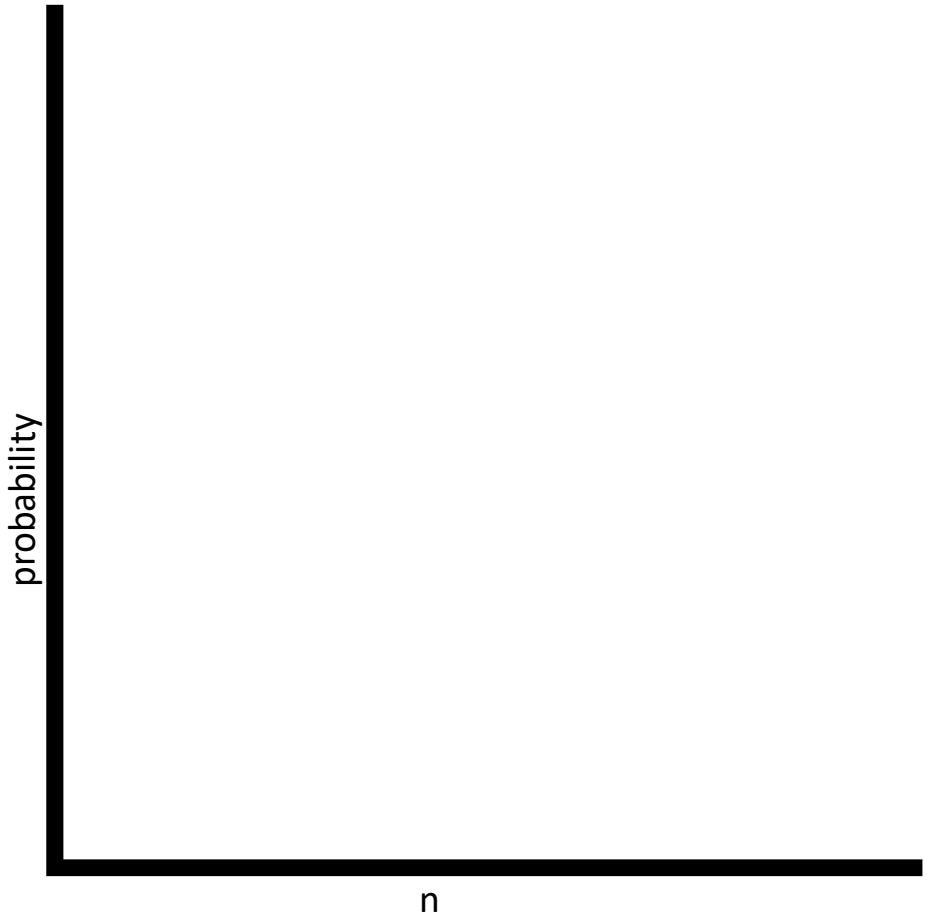
Diabetes
Measles
Measles
Stroke
Diabetes
Measles

Xq2gZZ
pg73Qq
pg73Qq
w5KL2z
Xq2gZZ
pg73Qq

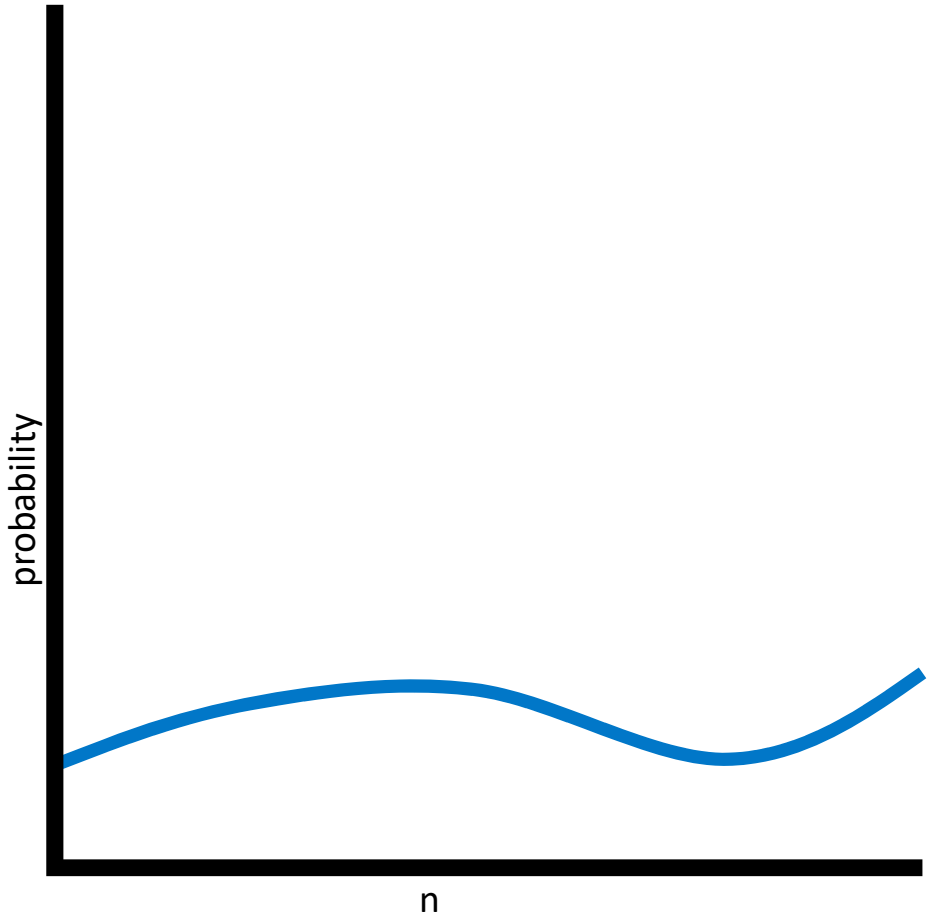
The database column of diseases, drawn independently according to some prior distribution δ on diseases

The deterministic encryption of the column, modeled as a random permutation (the “ideal object”)

Quantitative Information Flow Concepts

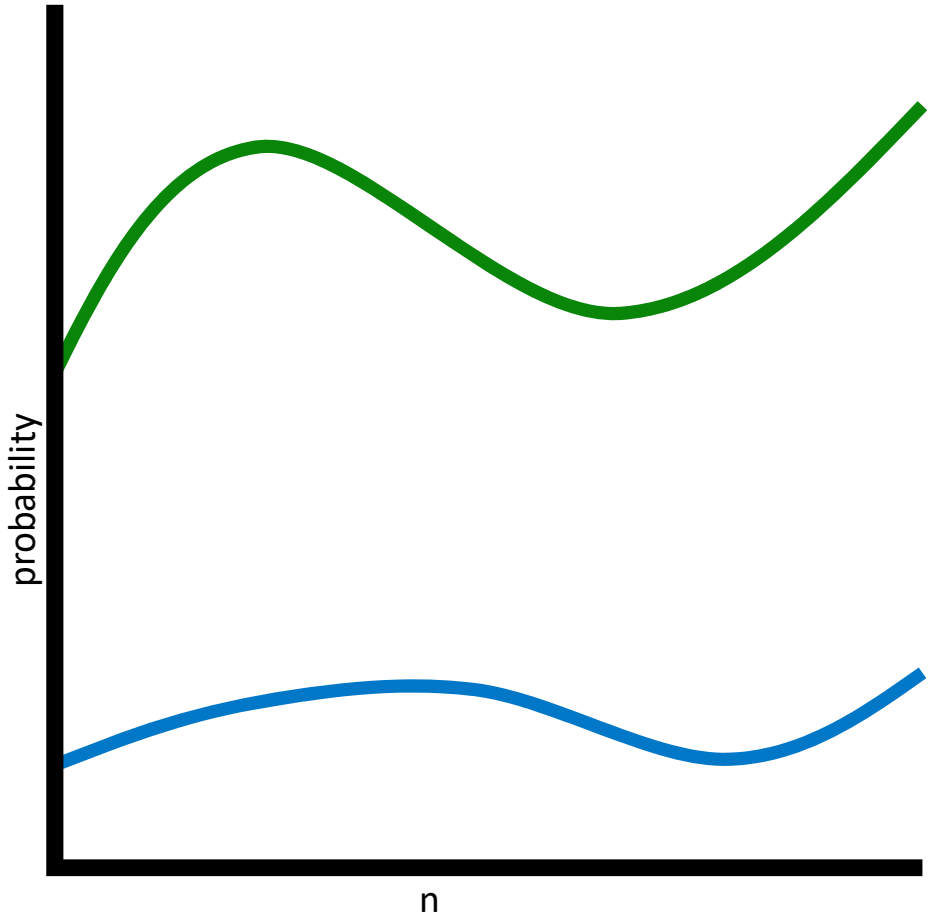


Quantitative Information Flow Concepts



Prior vulnerability:
Adversary's probability of accomplishing goal given only δ

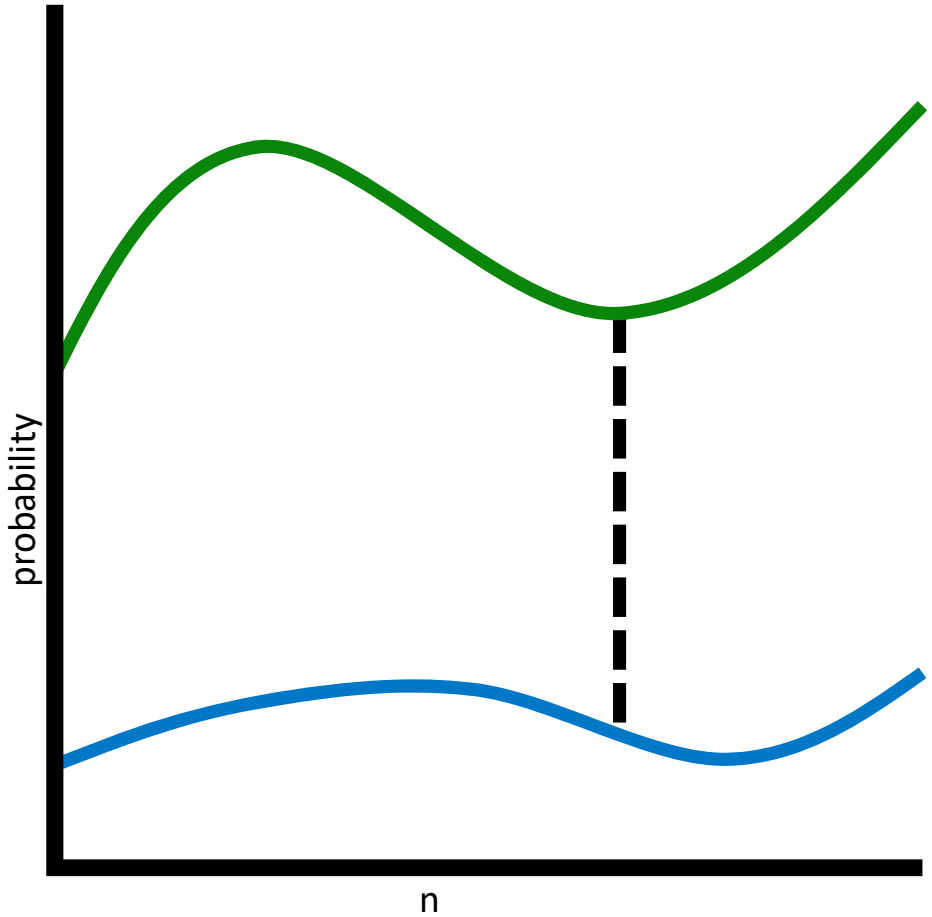
Quantitative Information Flow Concepts



Posterior vulnerability:
Adversary's probability of accomplishing goal given δ **and** output *Y*

Prior vulnerability:
Adversary's probability of accomplishing goal given only δ

Quantitative Information Flow Concepts



Posterior vulnerability:
Adversary's probability of accomplishing goal given δ **and** output *Y*

Leakage:
The difference between prior and posterior vulnerability

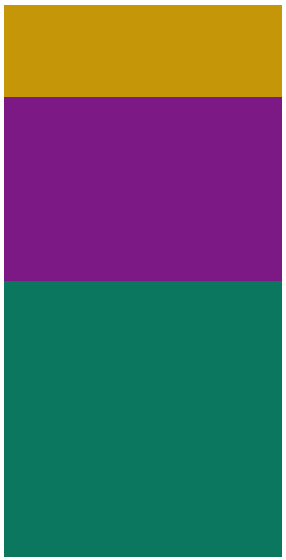
Prior vulnerability:
Adversary's probability of accomplishing goal given only δ

Intuition of Model

Disease	Probability δ
a	$1/2$
b	$1/3$
c	$1/6$

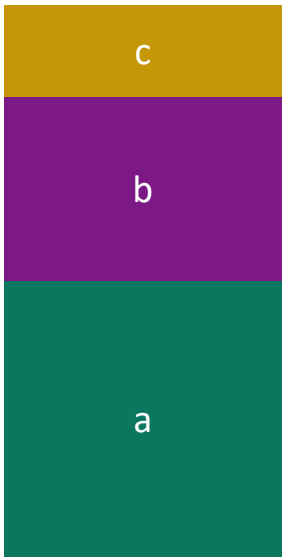
Intuition of Model

Disease	Probability δ
a	$1/2$
b	$1/3$
c	$1/6$



Intuition of Model

Disease	Probability δ
a	$1/2$
b	$1/3$
c	$1/6$

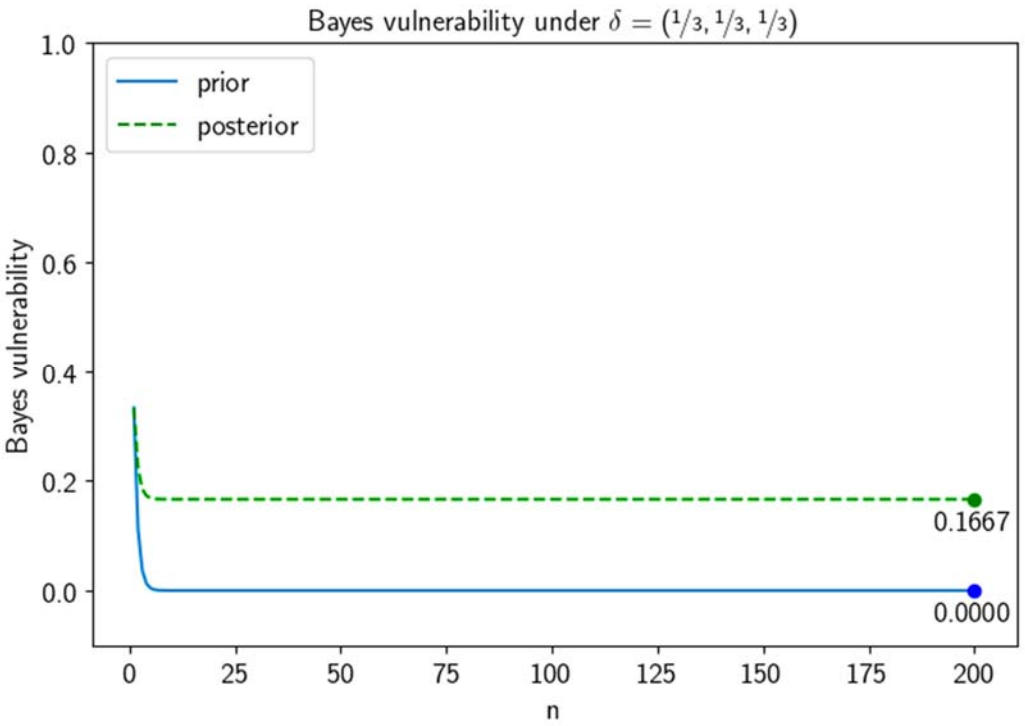


Results: Bayes Scenario

Goal: guess the entire secret in one try

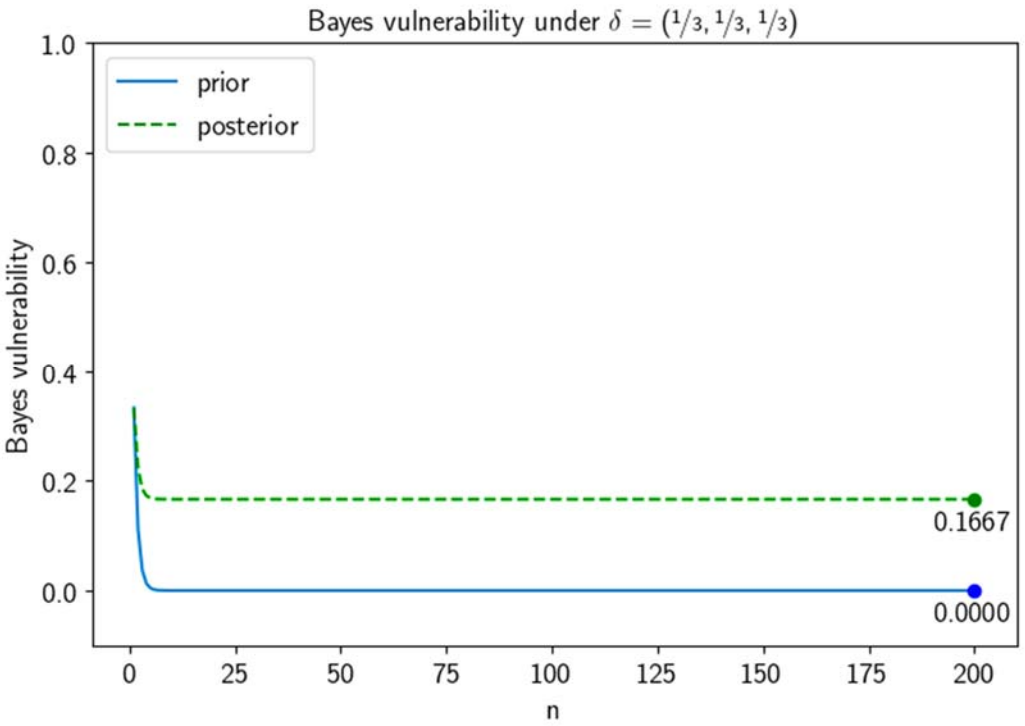
Results: Bayes Scenario

Goal: guess the entire secret in one try



Results: Bayes Scenario

Goal: guess the entire secret in one try

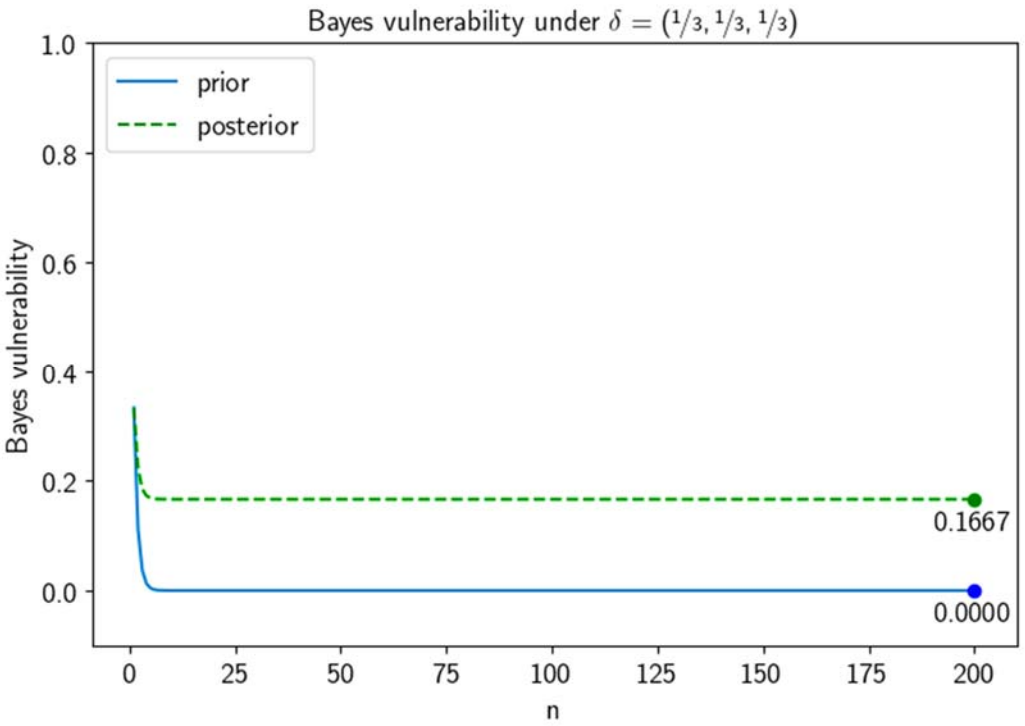


Prior Vulnerability:

When n = 1: ? $1/3$

Results: Bayes Scenario

Goal: guess the entire secret in one try



Prior Vulnerability:

When n = 1: ? $1/3$

When n is large: ? $1/3^n$

?

?

?

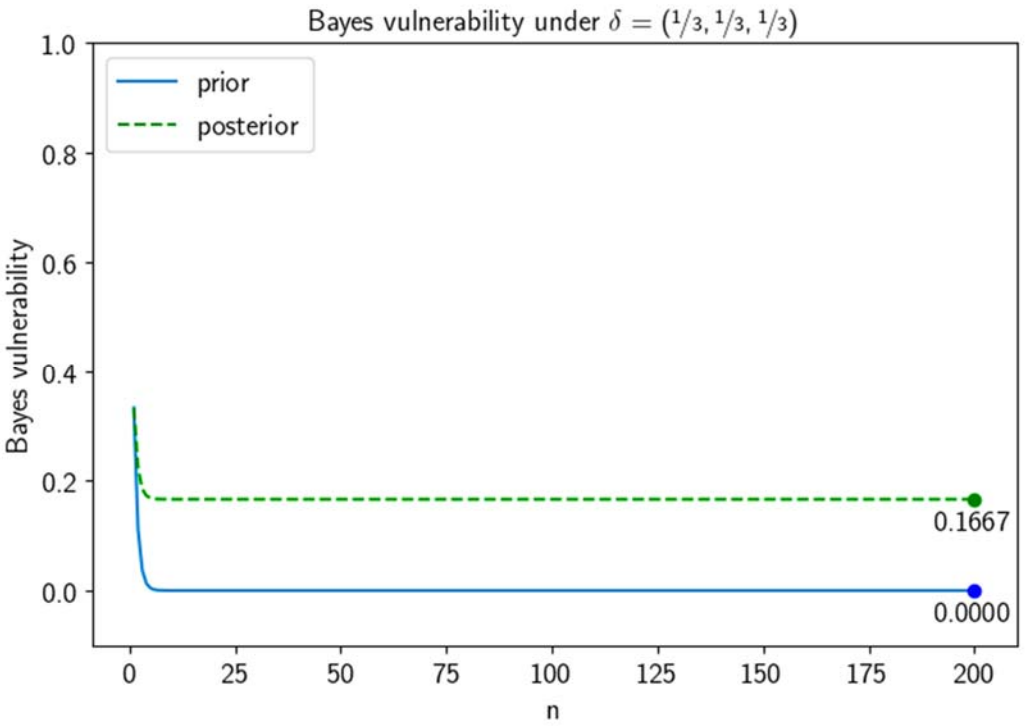
?

?

?

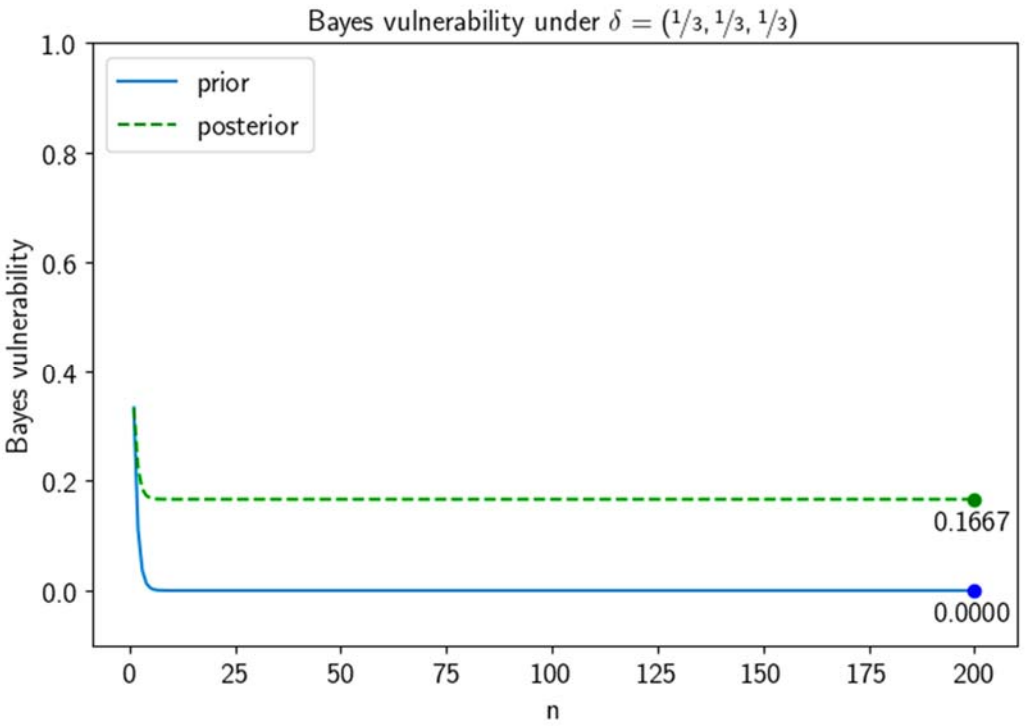
Results: Bayes Scenario

Goal: guess the entire secret in one try



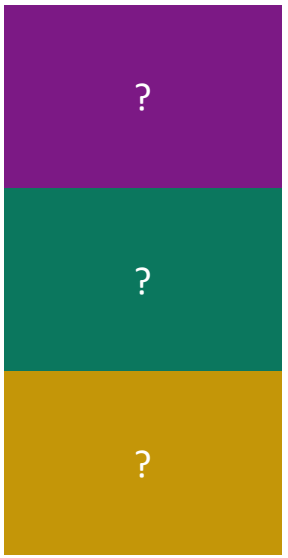
Results: Bayes Scenario

Goal: guess the entire secret in one try



Posterior Vulnerability:

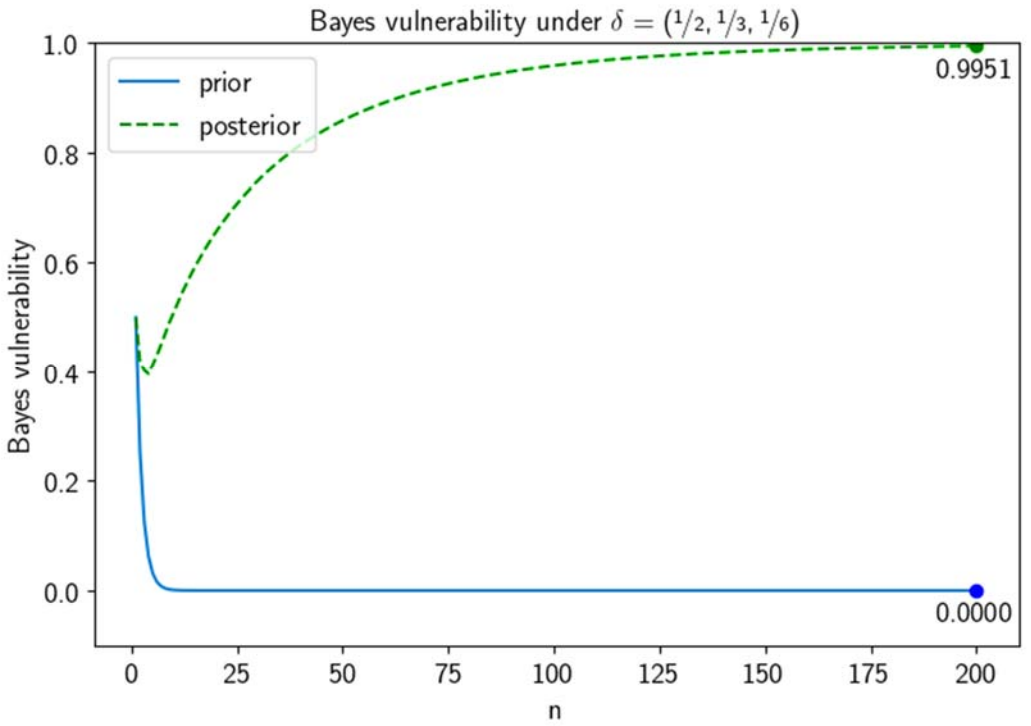
When n is large:



$1/6$

Results: Bayes Scenario

Goal: guess the entire secret in one try

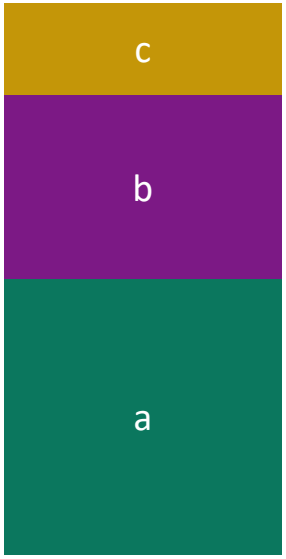


Results: Bayes Scenario

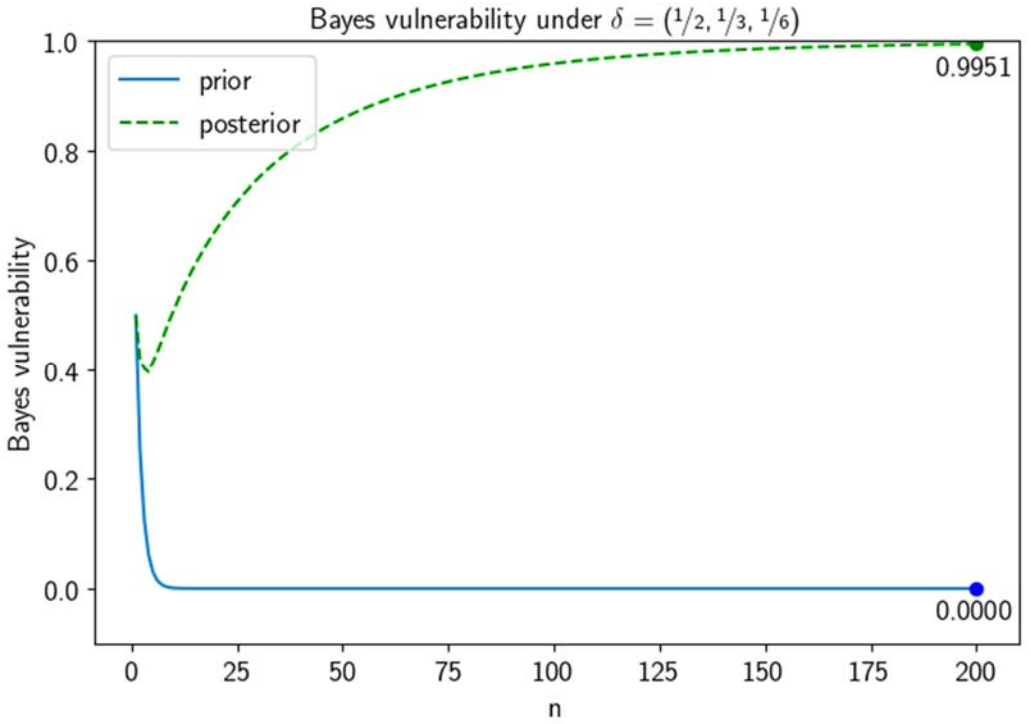
Goal: guess the entire secret in one try

Posterior Vulnerability:

When n is large:

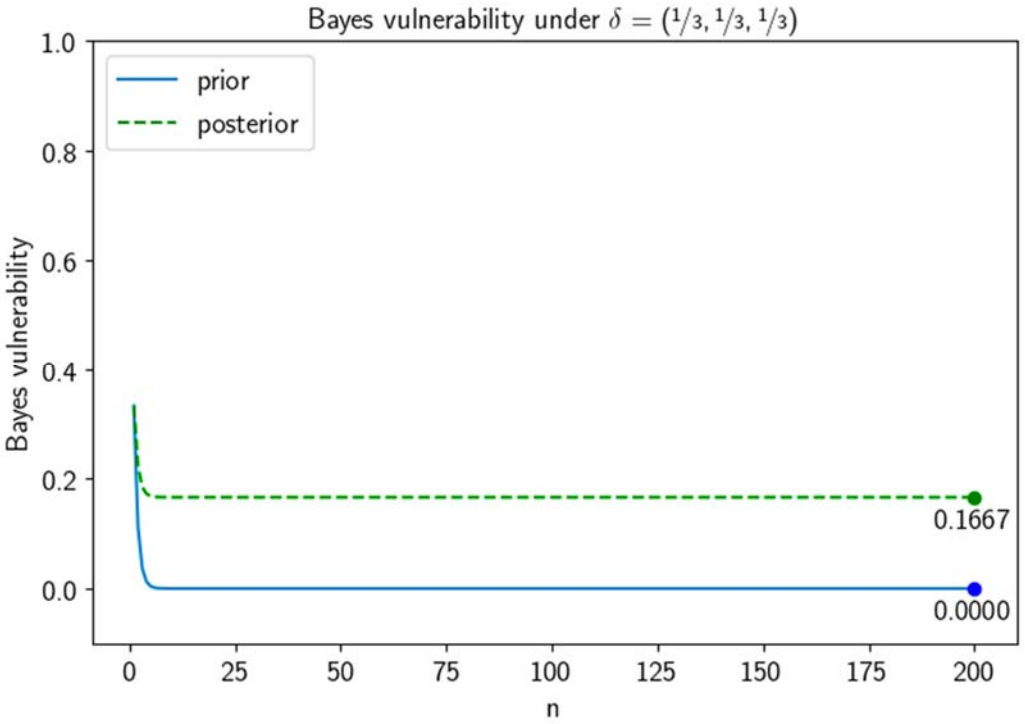


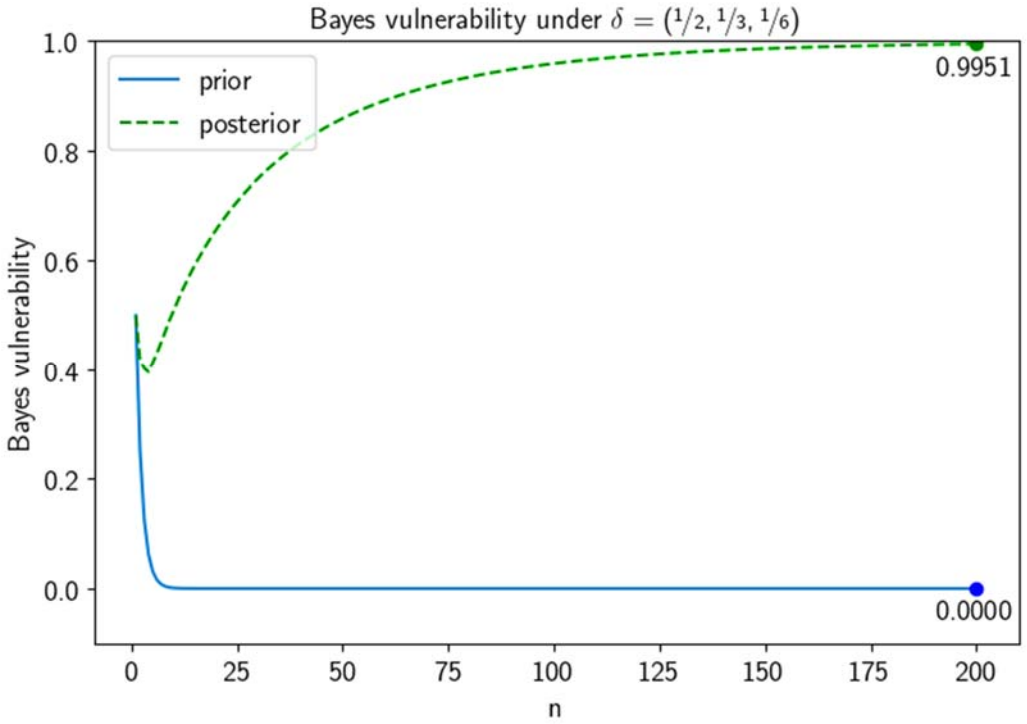
grows to 1



Results: Bayes Scenario

Goal: guess the entire secret in one try



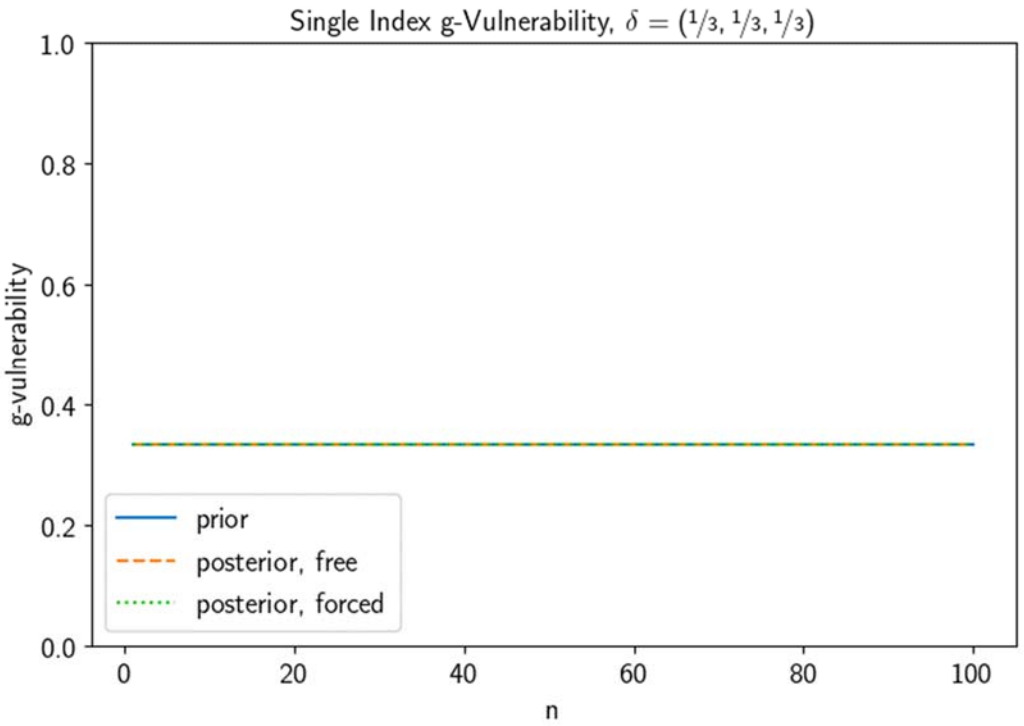


Results: Single Index Scenarios

Goals: (1) *free* to guess any patient's disease and (2) *forced* to guess a specified patient's disease

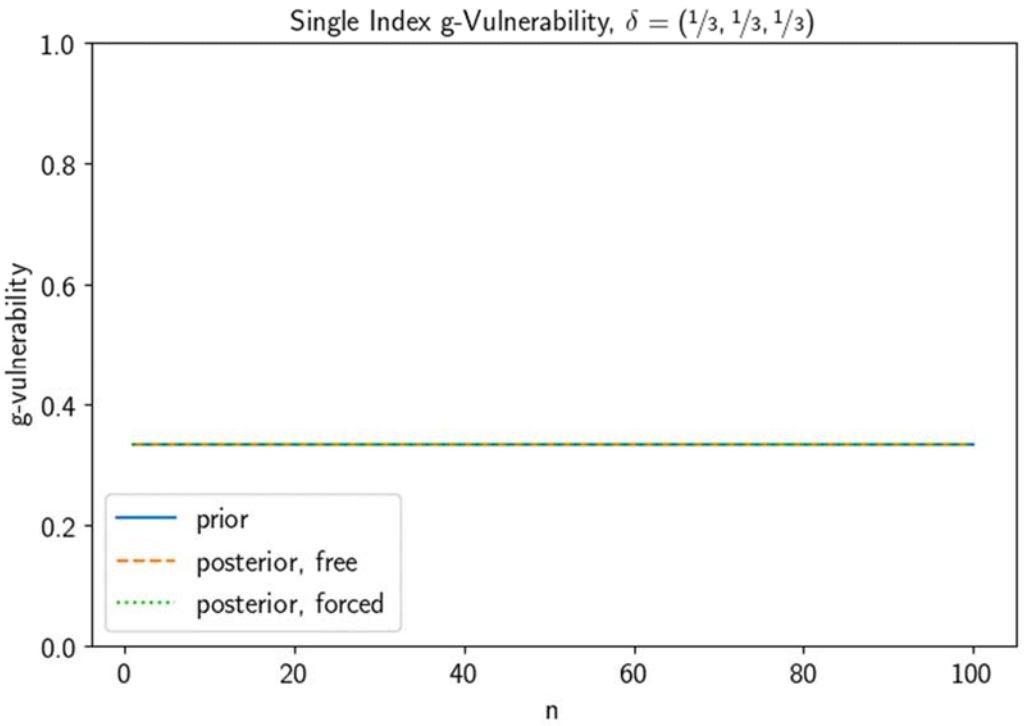
Results: Single Index Scenarios

Goals: (1) *free* to guess any patient's disease and (2) *forced* to guess a specified patient's disease

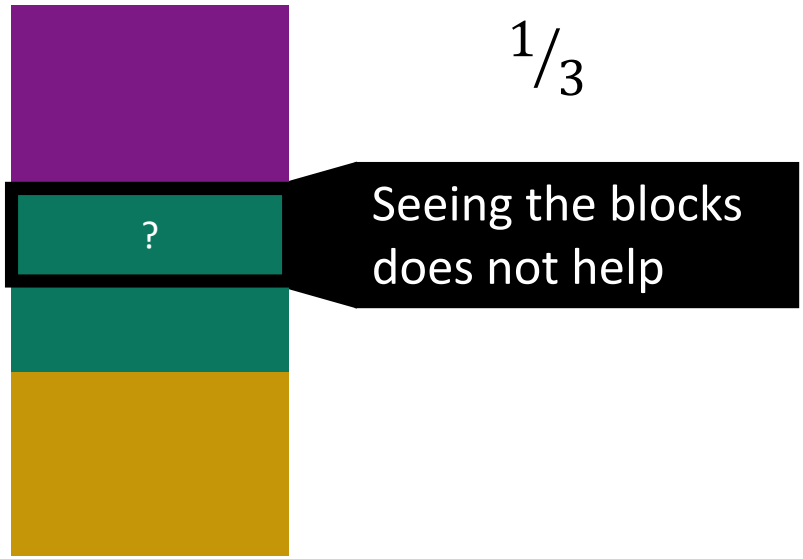


Results: Single Index Scenarios

Goals: (1) *free* to guess any patient's disease and (2) *forced* to guess a specified patient's disease

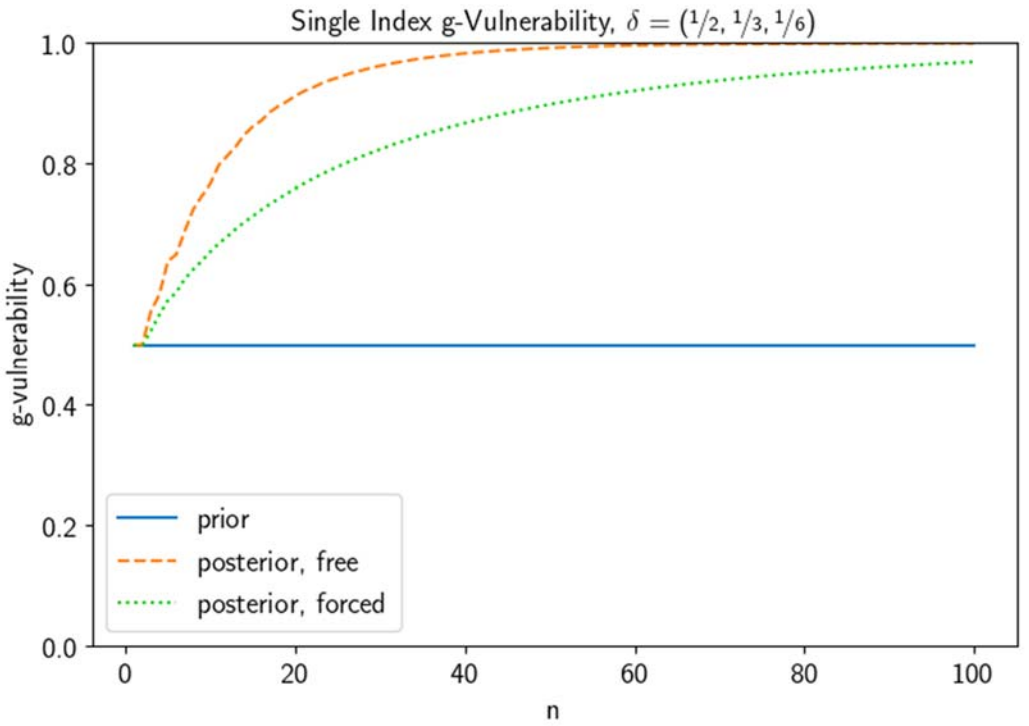


Posterior Vulnerability:



Results: Single Index Scenarios

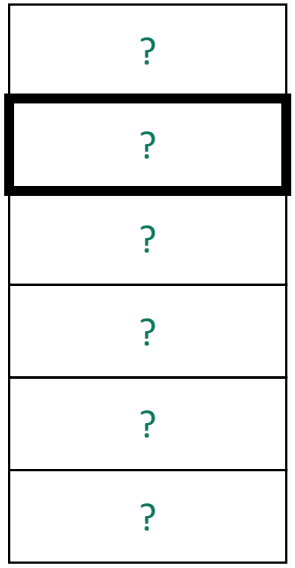
Goals: (1) *free* to guess any patient's disease and (2) *forced* to guess a specified patient's disease



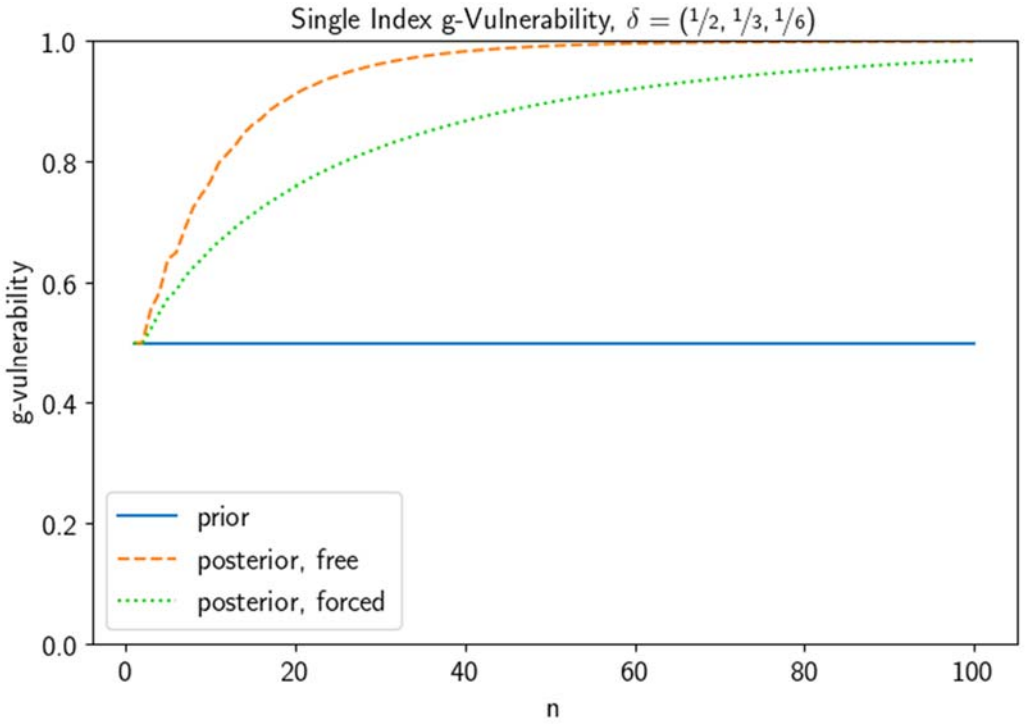
Results: Single Index Scenarios

Goals: (1) *free* to guess any patient's disease and (2) *forced* to guess a specified patient's disease

Prior Vulnerability:



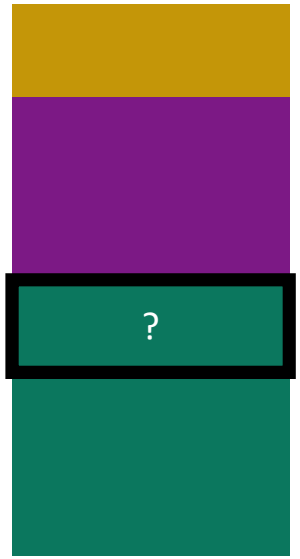
$1/2$



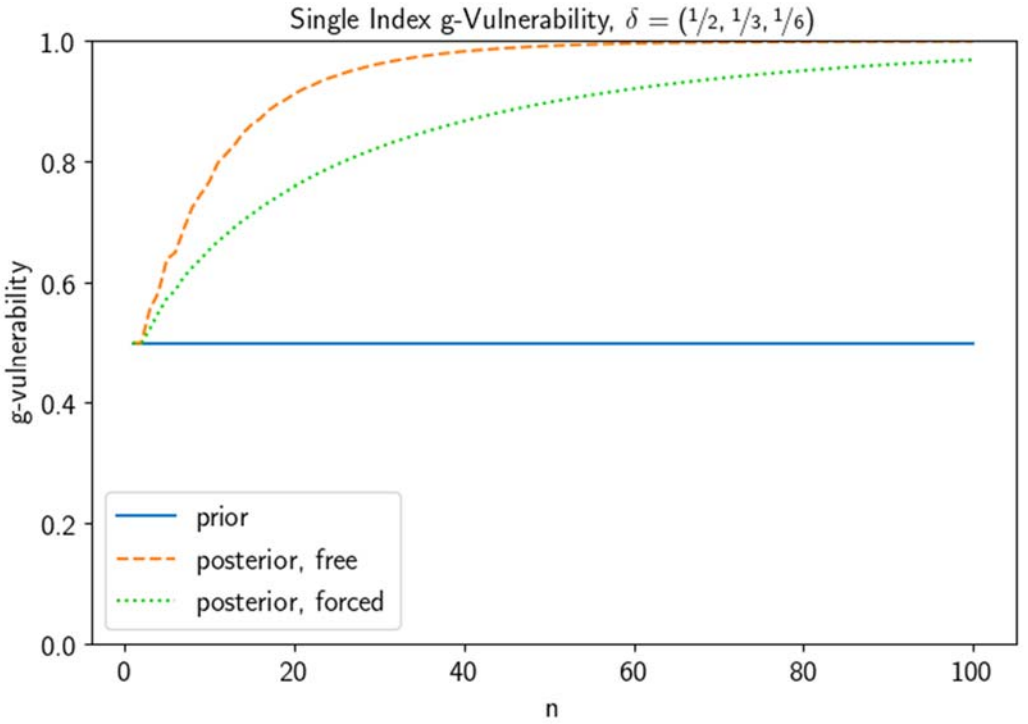
Results: Single Index Scenarios

Goals: (1) *free* to guess any patient's disease and (2) *forced* to guess a specified patient's disease

Posterior Vulnerability (free):



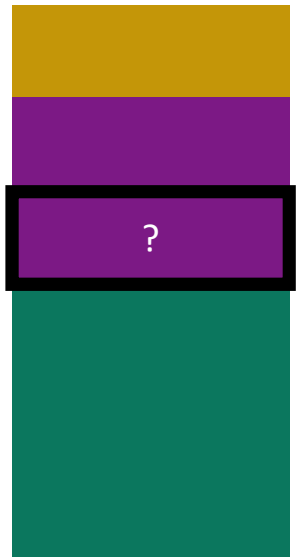
Goes up to 1



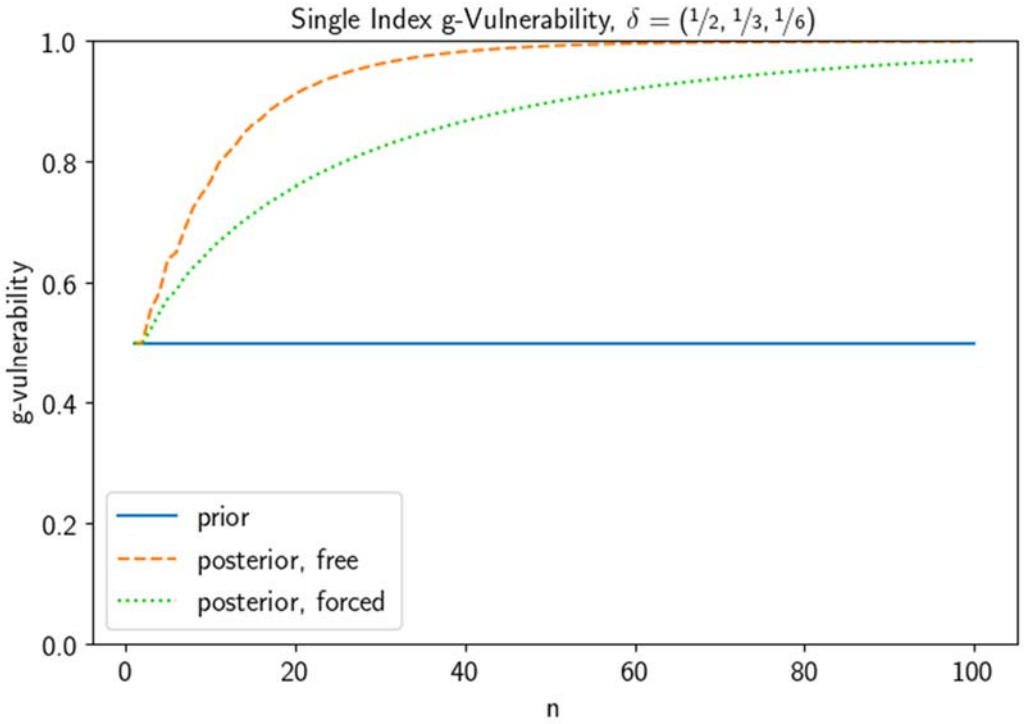
Results: Single Index Scenarios

Goals: (1) *free* to guess any patient's disease and (2) *forced* to guess a specified patient's disease

Posterior Vulnerability (forced):

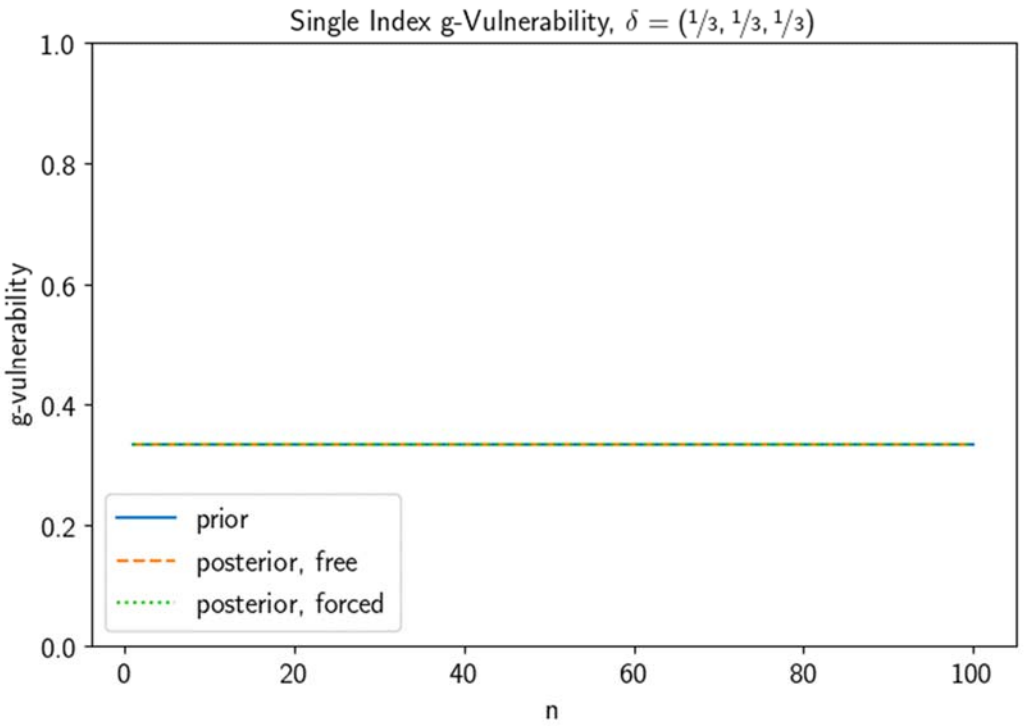


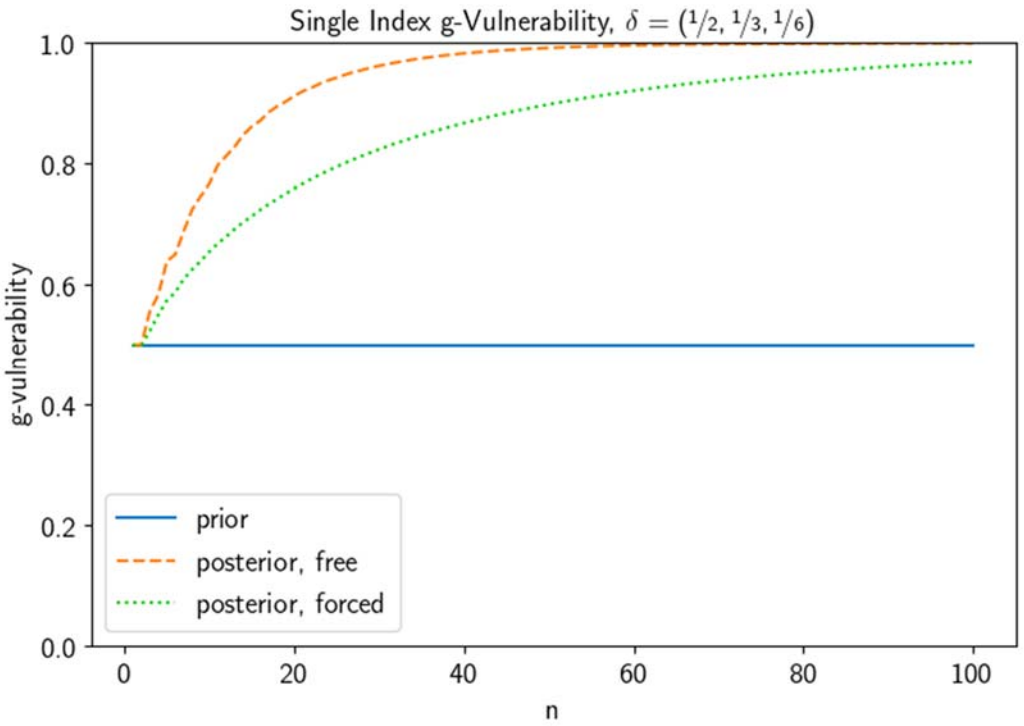
Grows slower

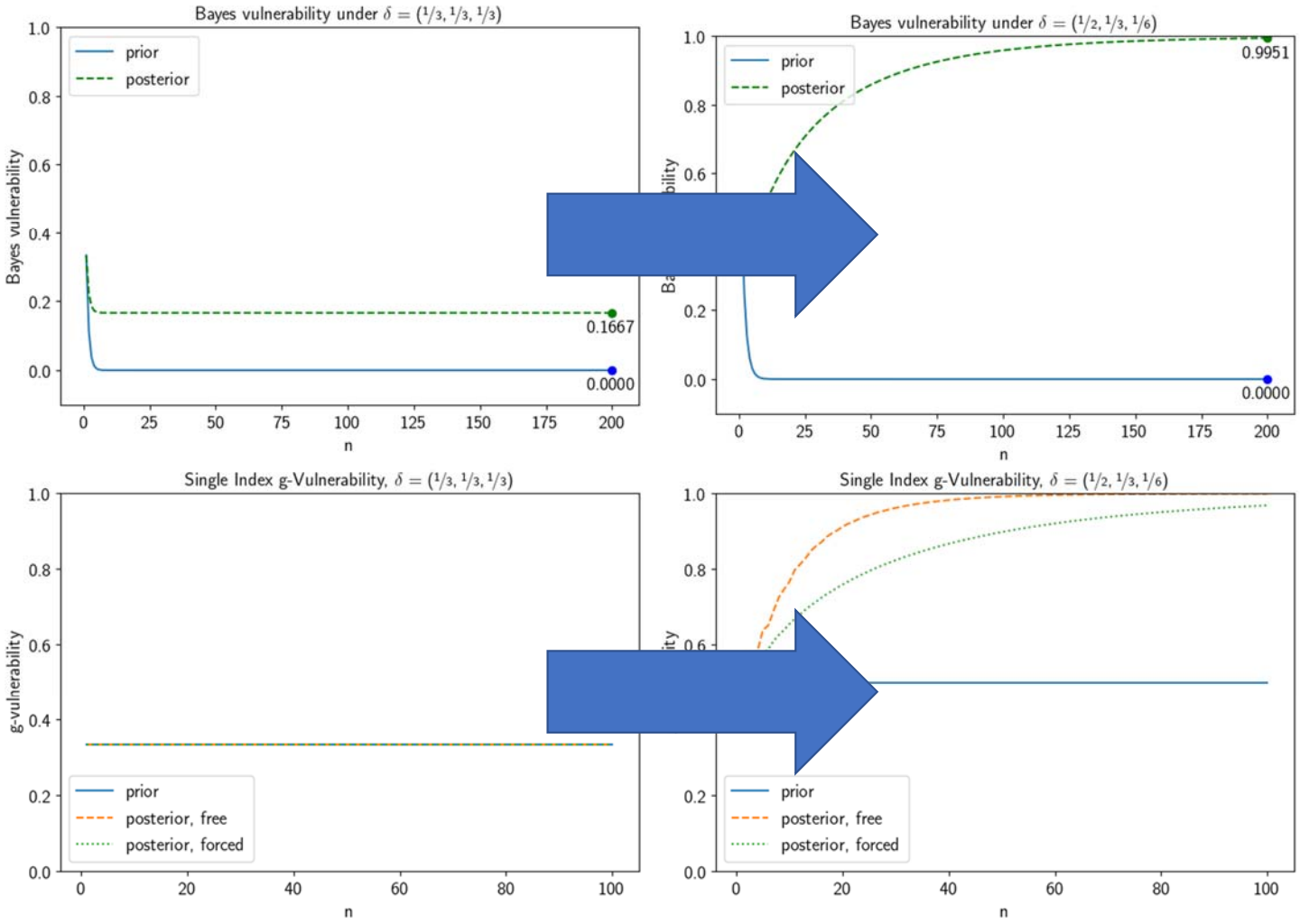


Results: Single Index Scenarios

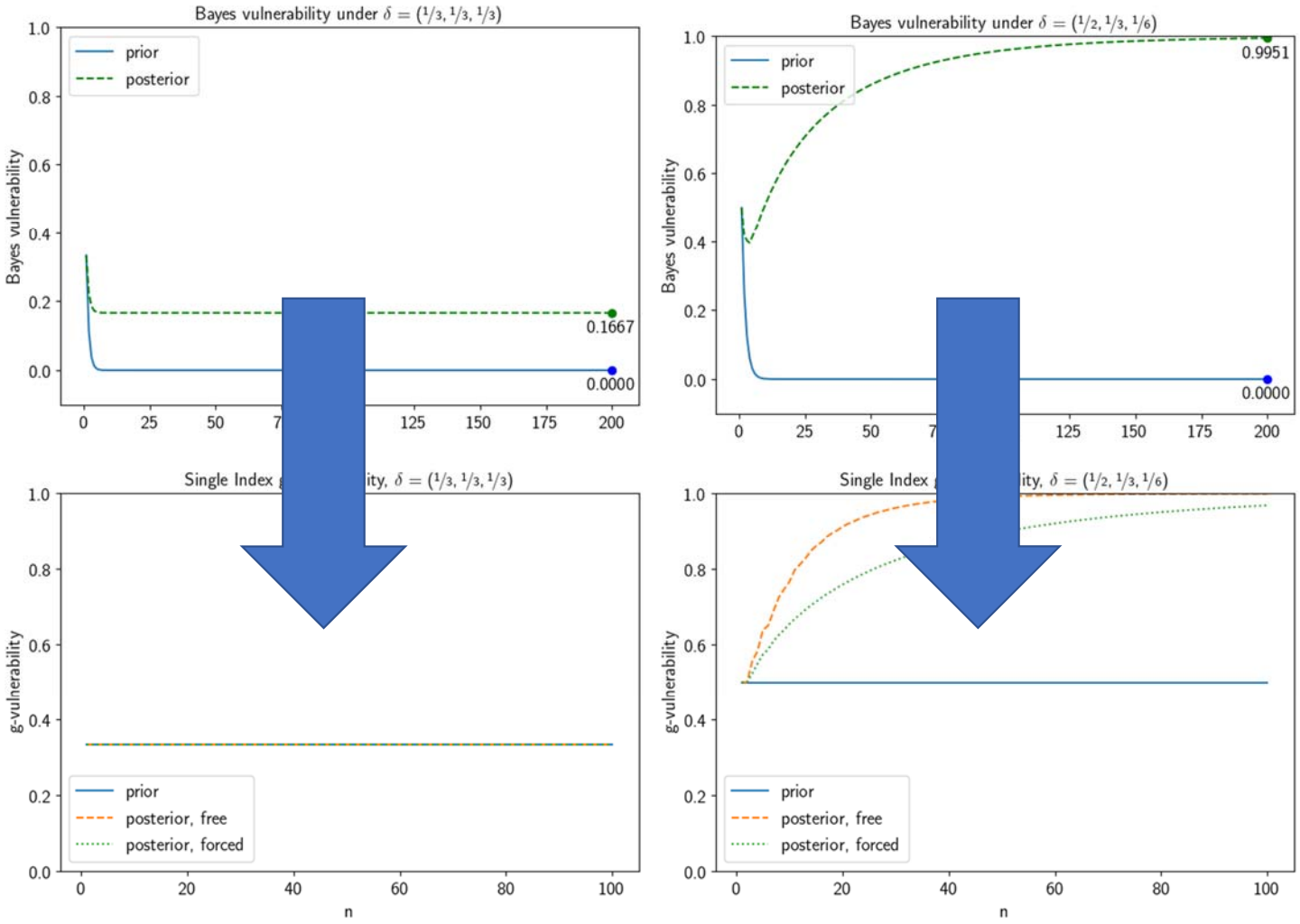
Goals: (1) *free* to guess any patient's disease and (2) *forced* to guess a specified patient's disease







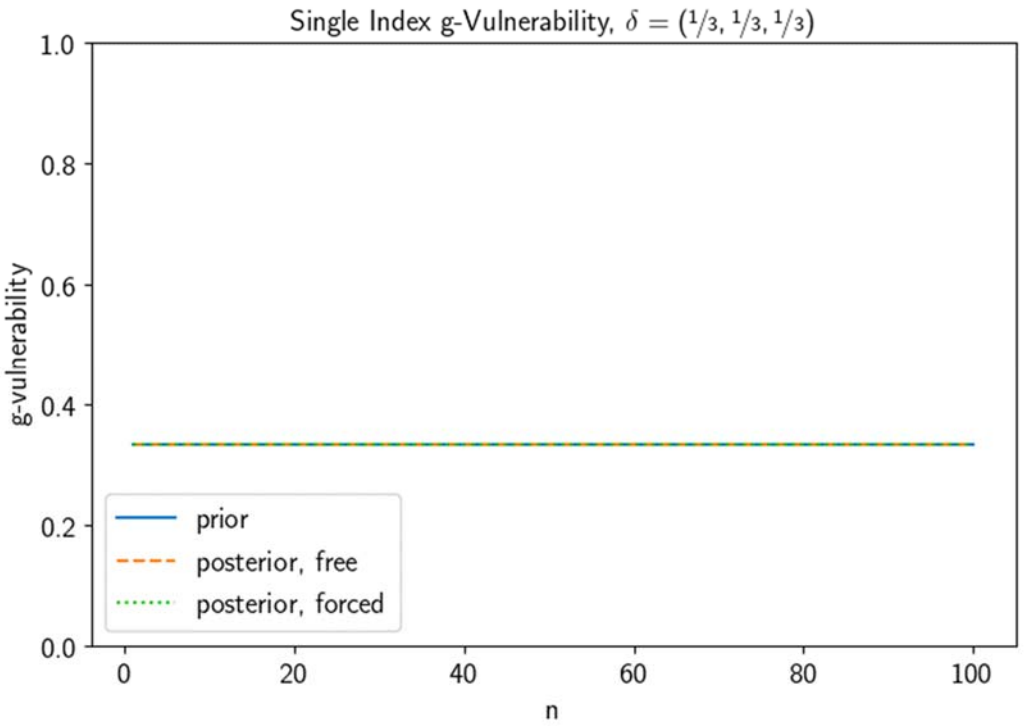
Leakage Depends on Prior and Operational Scenario

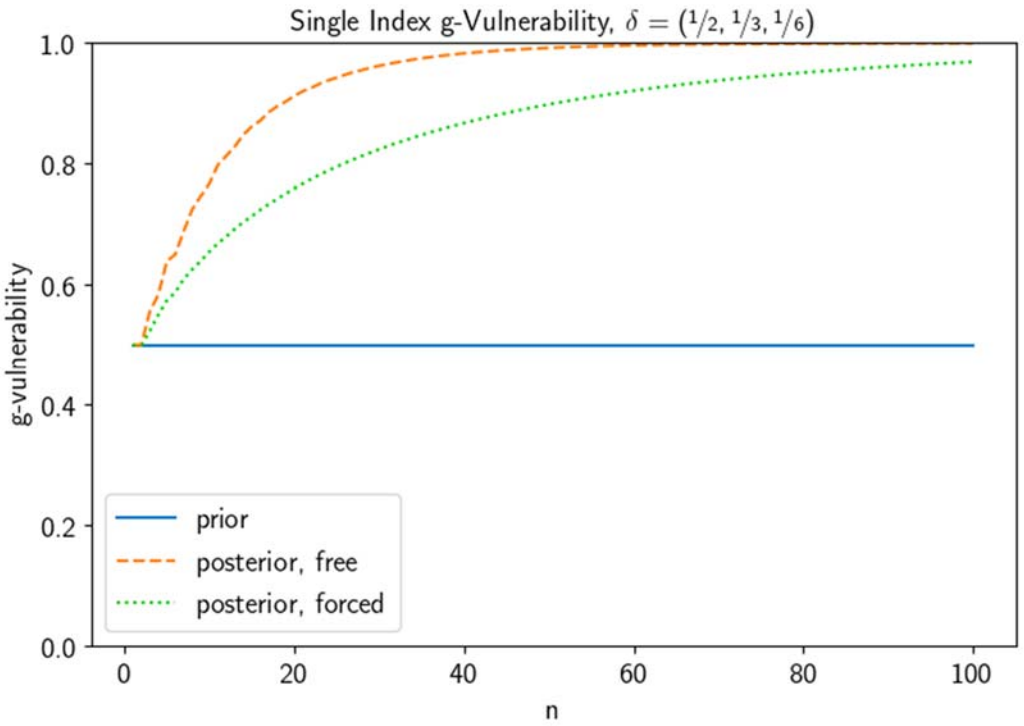


Leakage Depends on Prior and Operational Scenario

Results: Single Index Scenarios

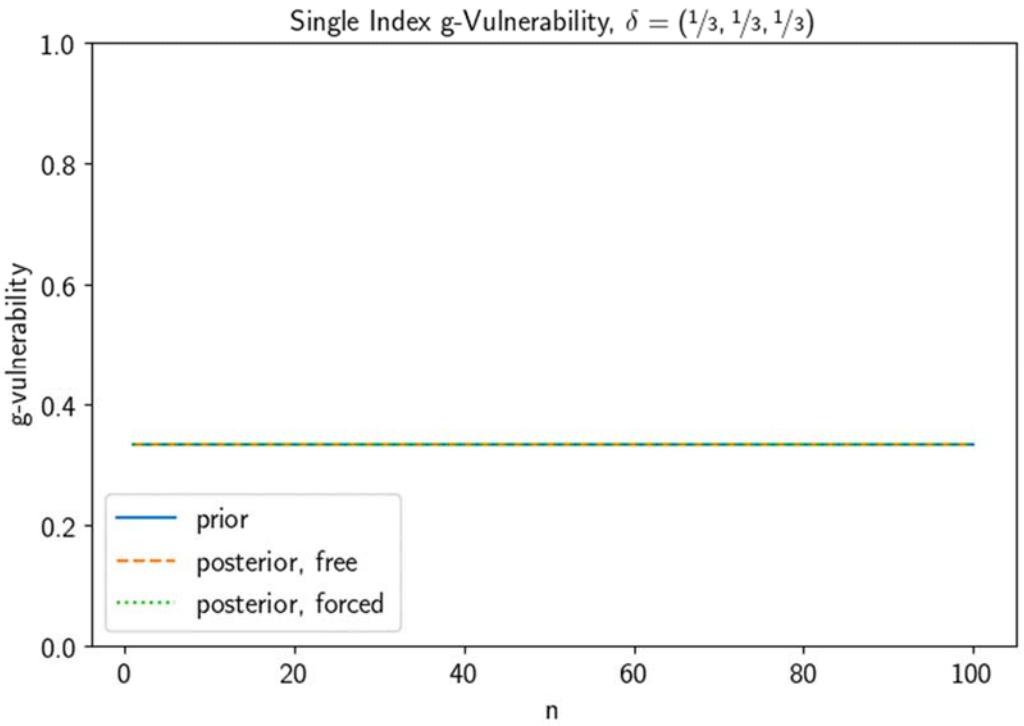
Goals: (1) *free* to guess any patient's disease and (2) *forced* to guess a specified patient's disease

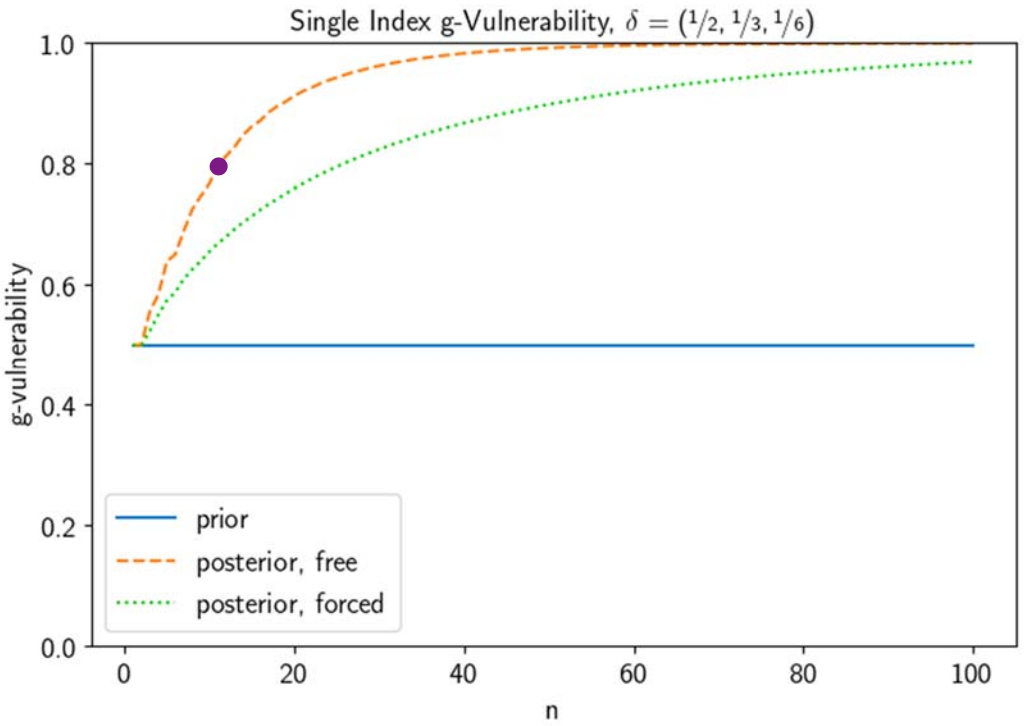




Results: Single Index Scenarios

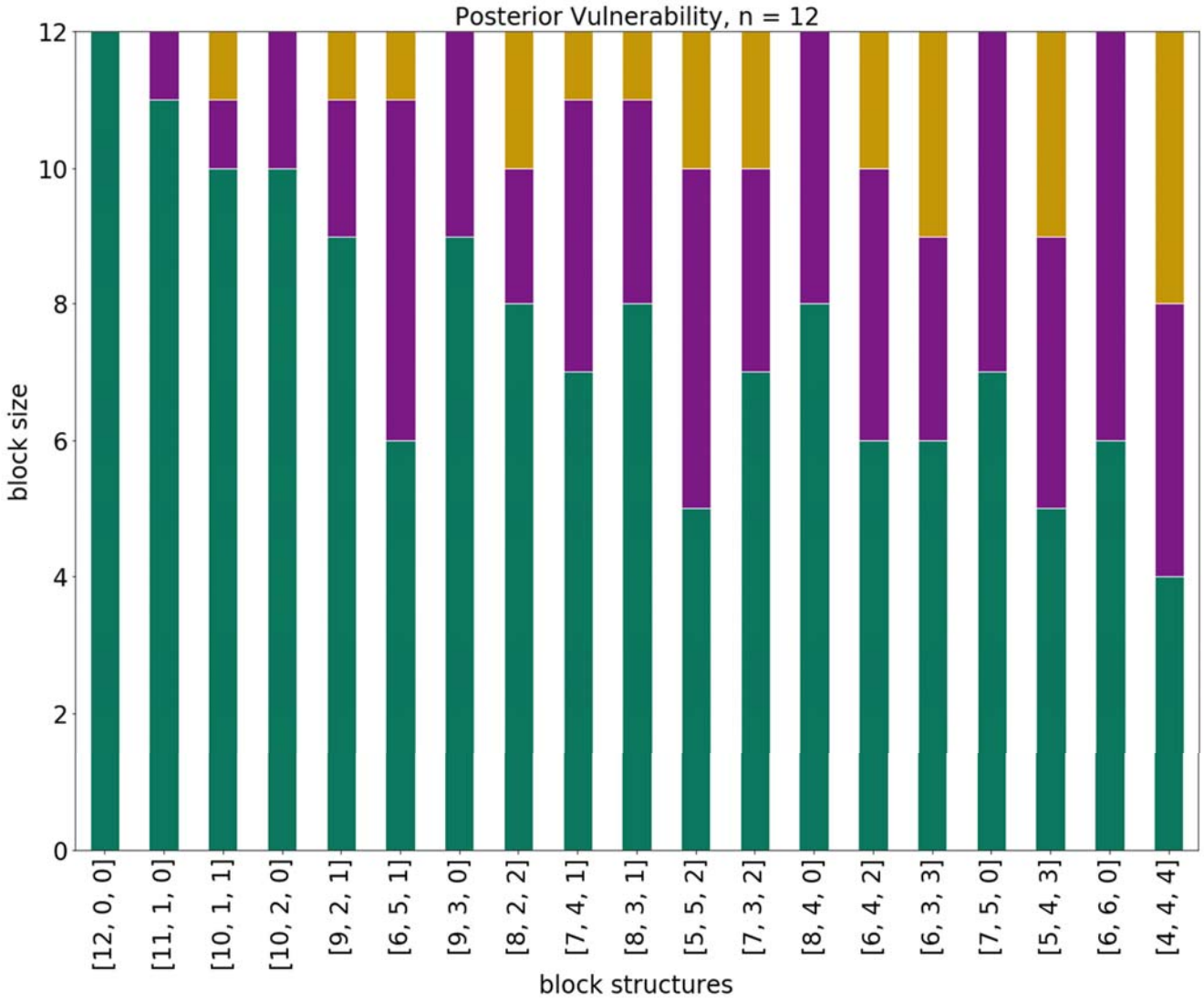
Goals: (1) *free* to guess any patient's disease and (2) *forced* to guess a specified patient's disease





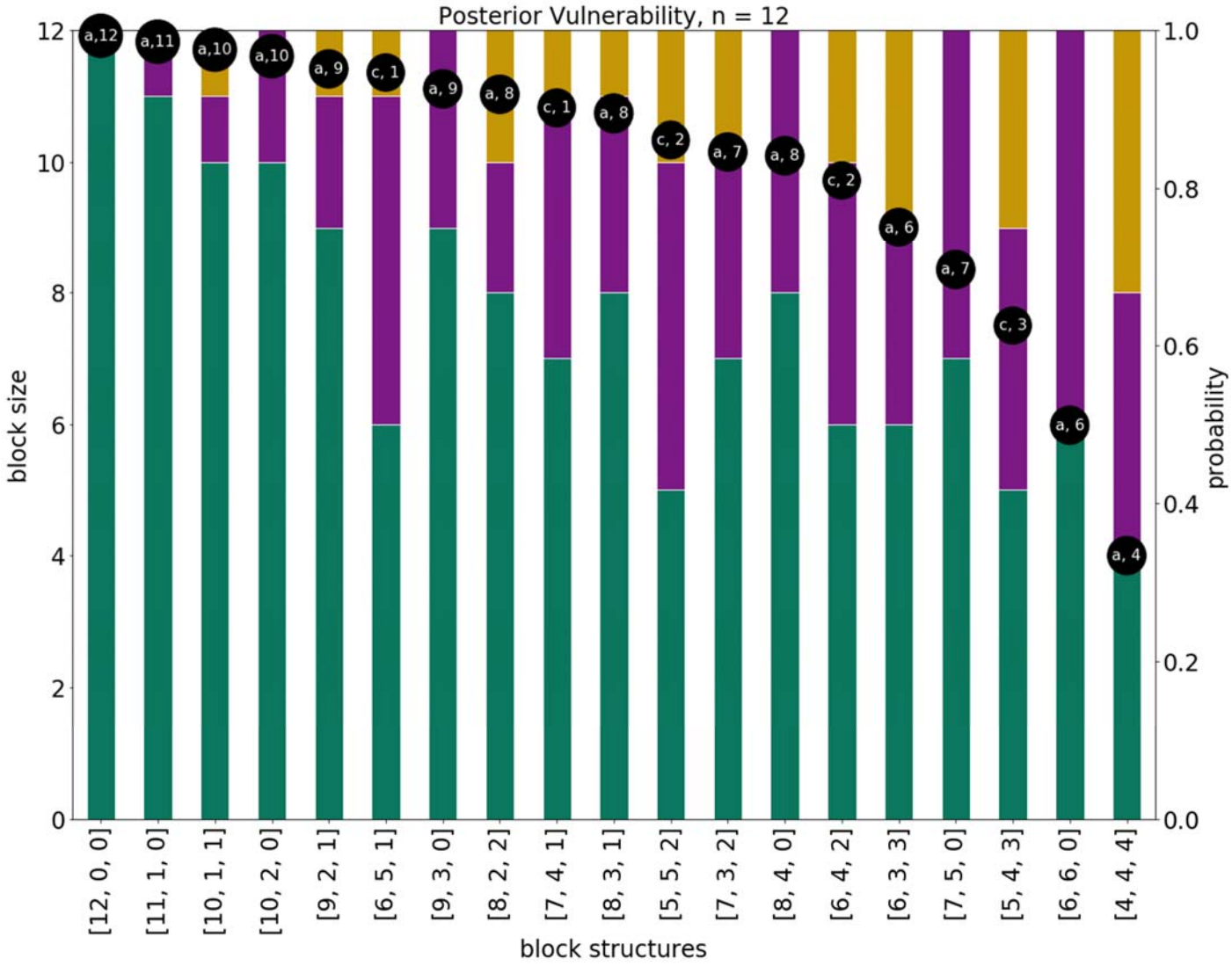
An In Depth View

- 19 possible block structures



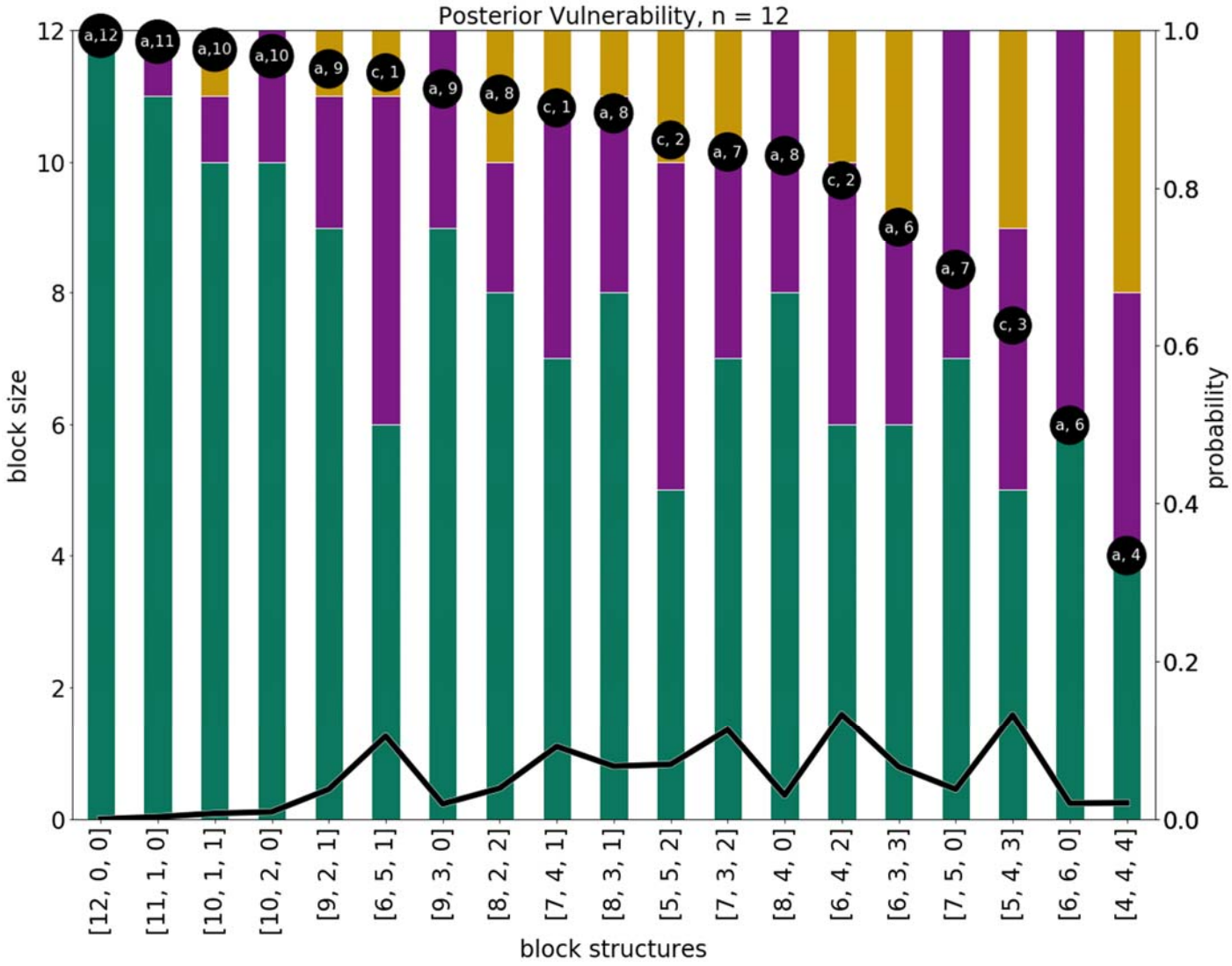
An In Depth View

- 19 possible block structures
- Dots: the best guess and her probability of being correct



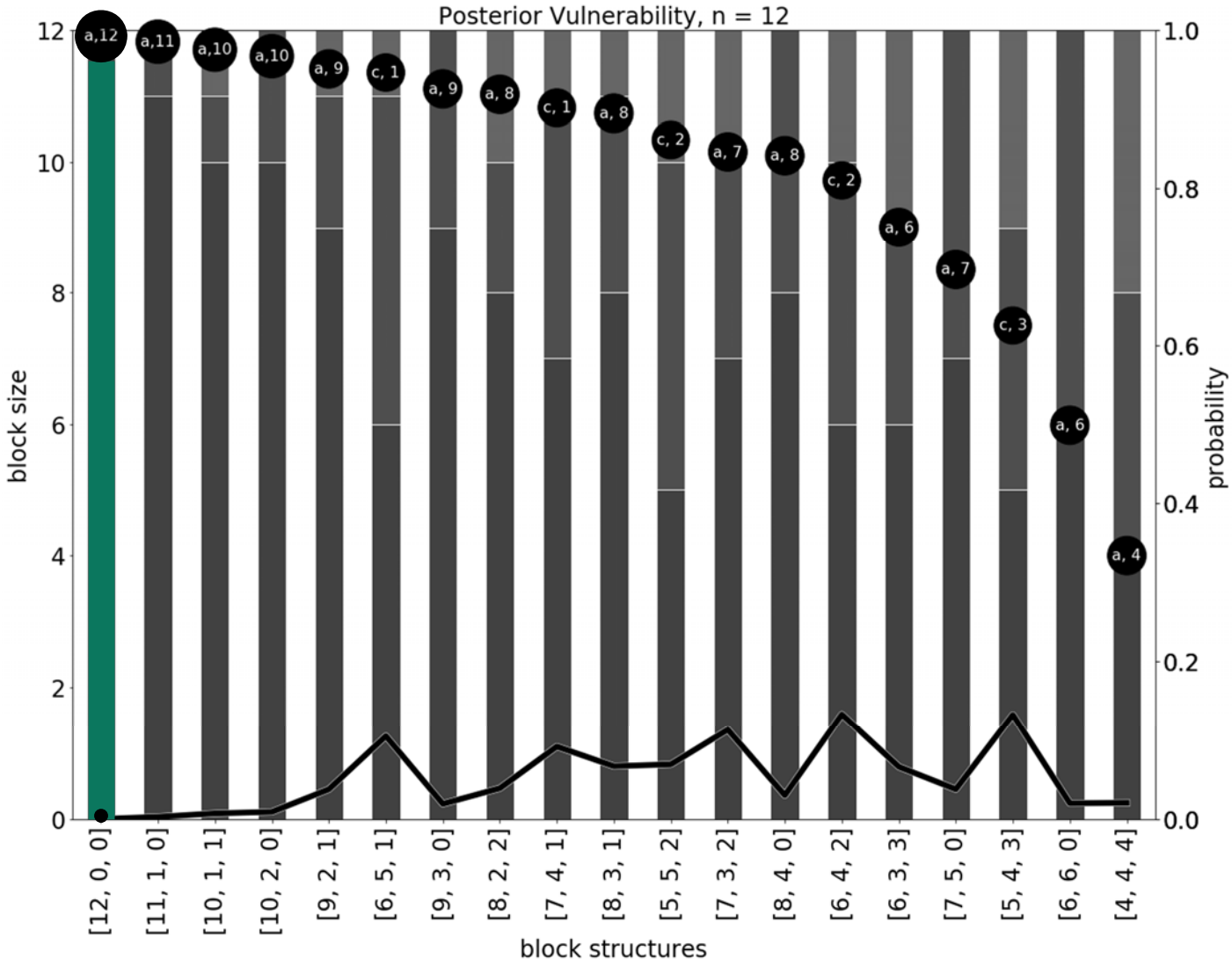
An In Depth View

- 19 possible block structures
- Dots: the best guess and her probability of being correct
- Line: the probability the block structure will occur



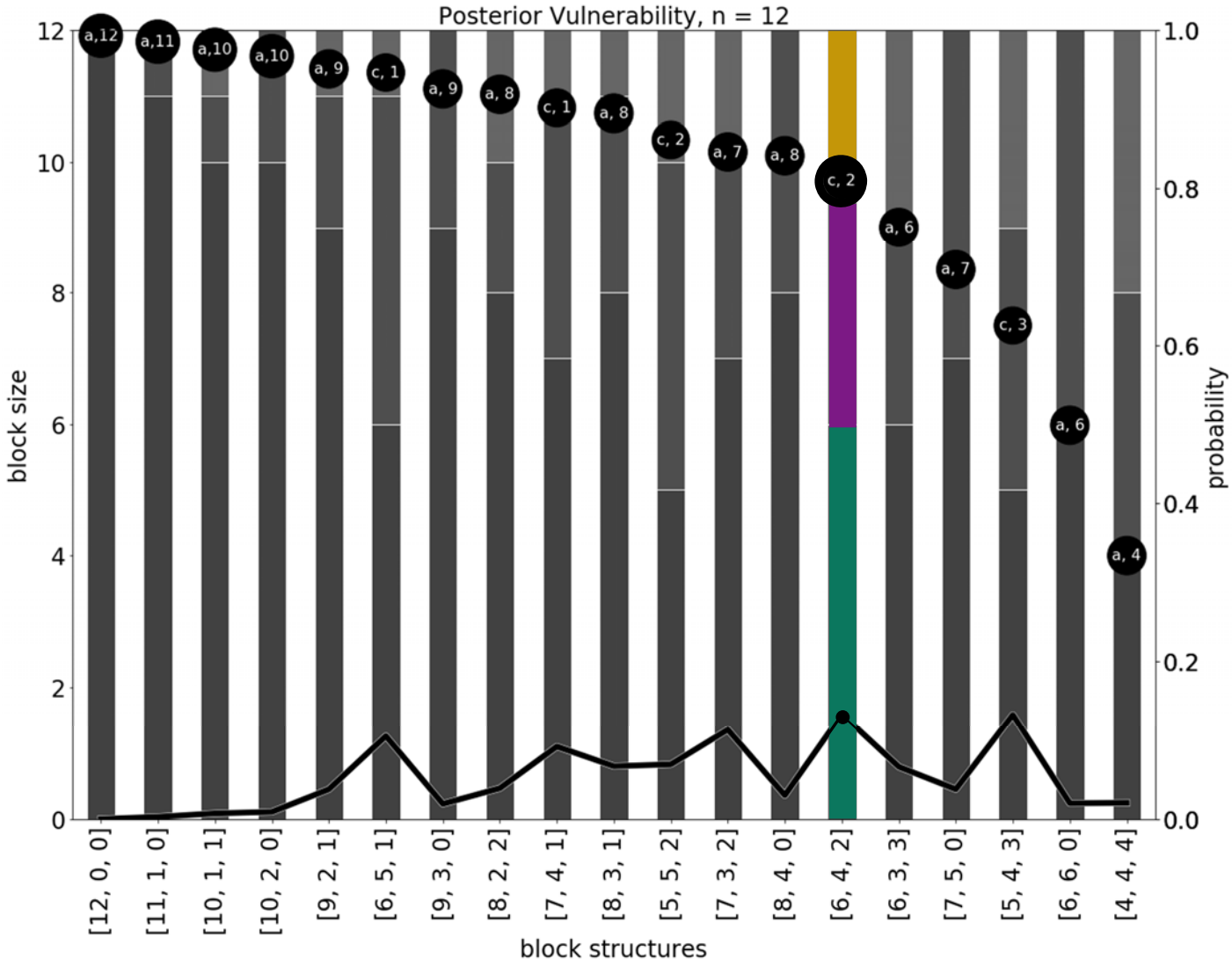
An In Depth View

- 19 possible block structures
- Dots: the best guess and her probability of being correct
- Line: the probability the block structure will occur



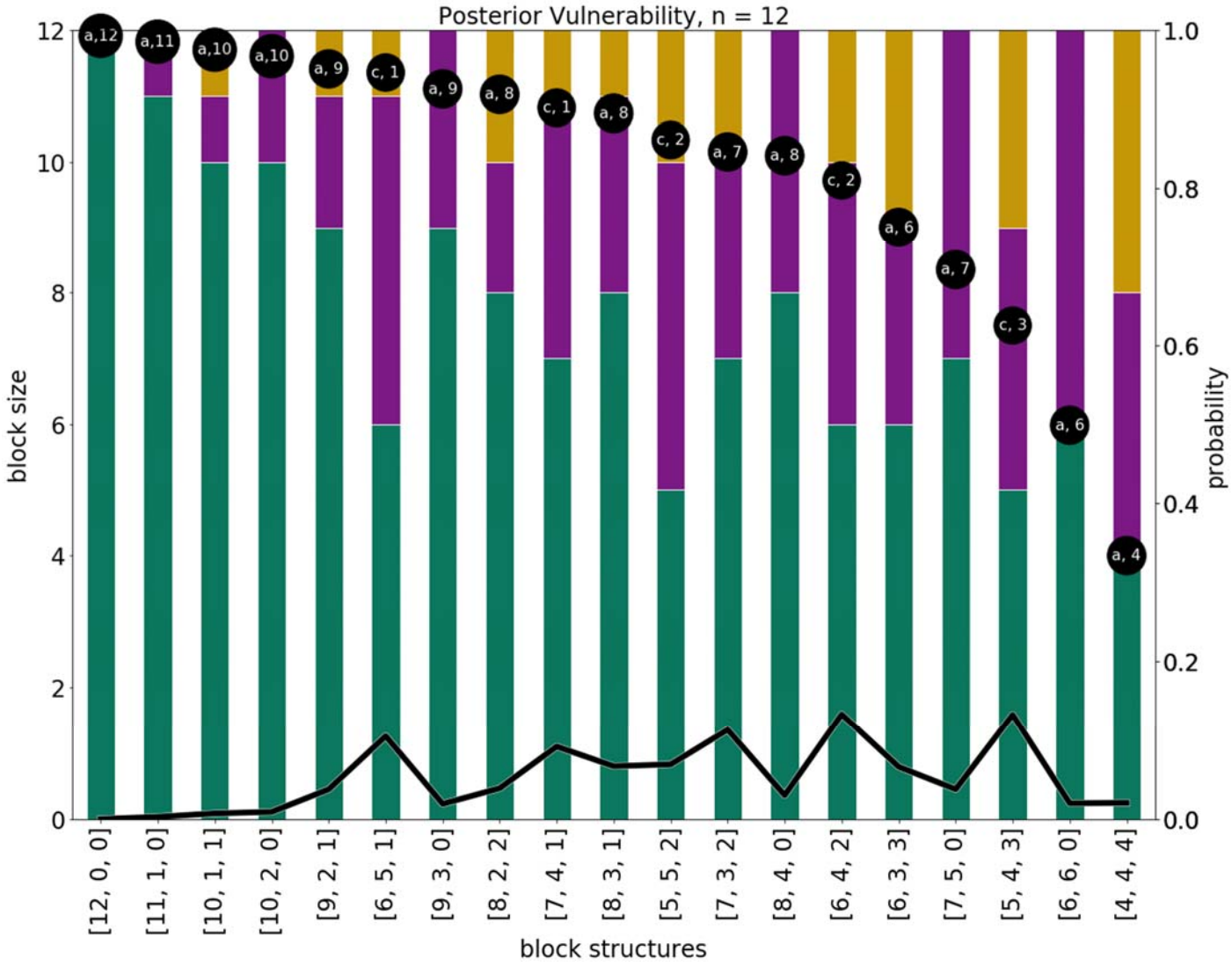
An In Depth View

- 19 possible block structures
- Dots: the best guess and her probability of being correct
- Line: the probability the block structure will occur



An In Depth View

- 19 possible block structures
- Dots: the best guess and her probability of being correct
- Line: the probability the block structure will occur
- **Posterior vulnerability: ~0.813**



Contributions

Revealed that there are scenarios where deterministic encryption is not safe even under a uniform prior.

Demonstrated a novel security framework by coupling the provable security approach of modern cryptography with QIF theory.

Illustrated that there is no one ‘right’ way to quantify leakage. Information flow depends on the operational scenario.