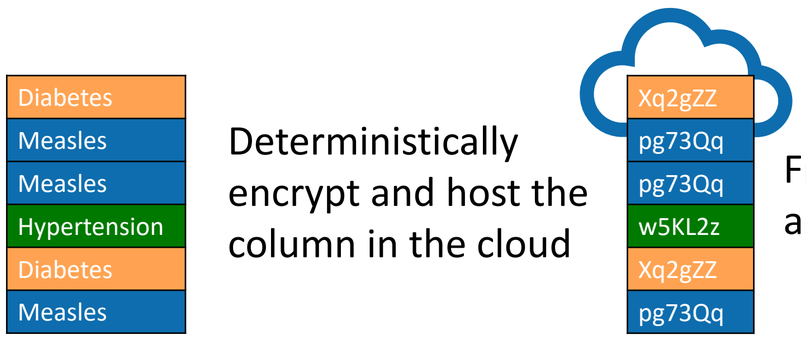
Quantifying Information Leakage in Searchable Encryption

PI Geoffrey Smith, Florida International University
Presented by Mireya Jurado

EAGER: Collaborative: CNS-1749014
(with PI Alexandra Boldyreva, Georgia Tech, CNS-1749069)

Challenge

- Goal: store sensitive data in the cloud
- Approach: encrypted databases balance security and functionality



Key question: How much sensitive information is leaked?

Approach: Quantitative Information Flow

- **Secret** X has value known to the adversary only as a **prior probability distribution** π
- **Channel** C probabilistically maps secret input X to observable output Y
- C maps prior π to a **hyper-distribution** [π ⊳ C], which is a **distribution on posterior distributions**

π	C	y_1	y_2	y_3	y_4
$1/4$	x_1	$1/2$	$1/2$	0	0
$1/2$	x_2	0	$1/4$	$1/2$	$1/4$
$1/4$	x_3	$1/2$	$1/3$	$1/6$	0

⇨

J	y_1	y_2	y_3	y_4
x_1	$1/8$	$1/8$	0	0
x_2	0	$1/8$	$1/4$	$1/8$
x_3	$1/8$	$1/12$	$1/24$	0

⇨

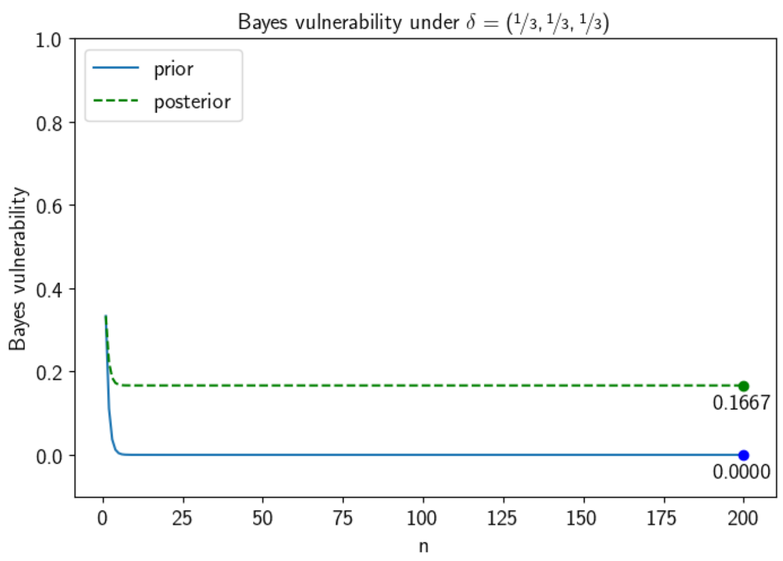
[π⊳C]	$1/4$	$1/3$	$7/24$	$1/8$
x_1	$1/2$	$3/8$	0	0
x_2	0	$3/8$	$6/7$	1
x_3	$1/2$	$1/4$	$1/7$	0

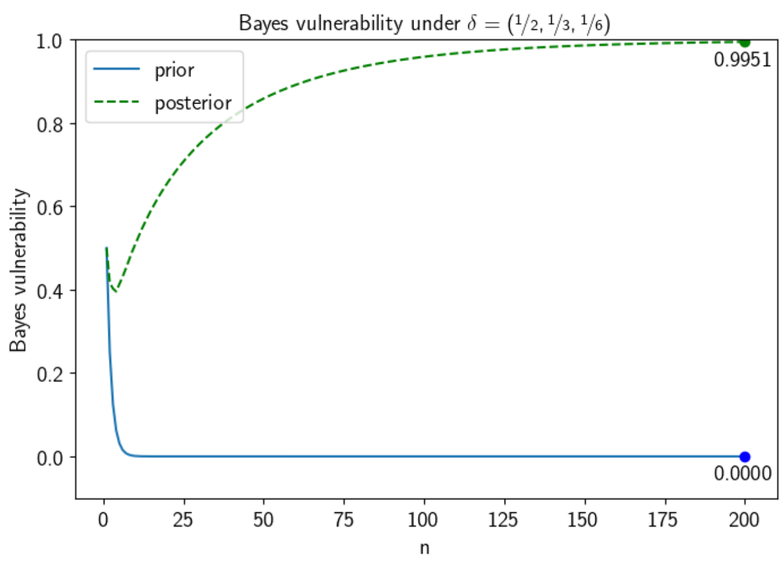
- **Prior** and **posterior vulnerability**: the threat to the secret **before** and **after** the channel is run
- **Leakage:** the difference between posterior & prior vulnerability

Deterministic Encryption Analysis

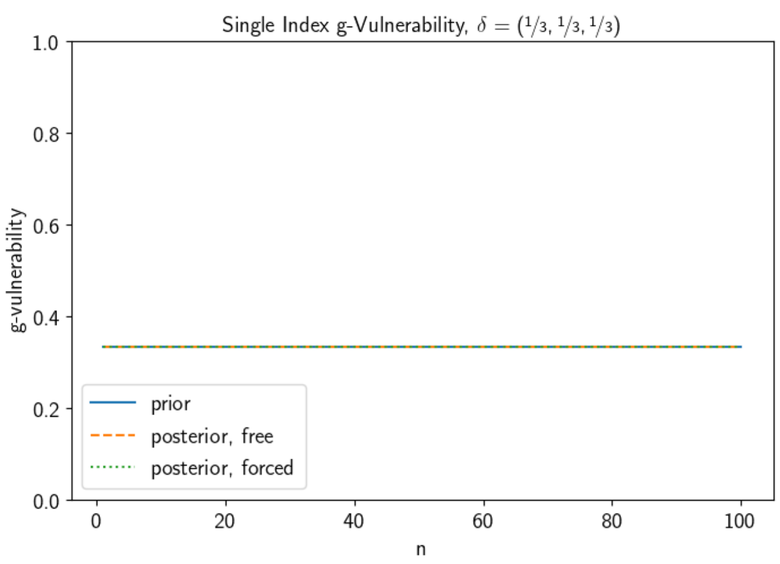
- Cryptography assumes a **computationally-bounded** adversary, while QIF is **information theoretic**.
- But QIF can analyze the cryptographic **ideal object**. (E.g. a block cipher is modeled as a random permutation.)

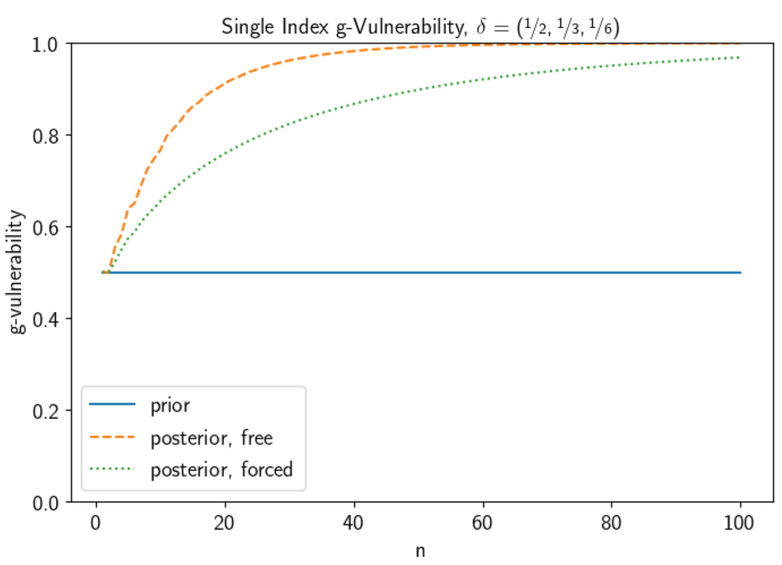
Bayes Scenario: Guess the entire secret column in one try





Single Index Scenarios: (1) *Free* to guess any patient's disease and (2) *forced* to guess a specified patient's disease





Future Directions

- Refinement order among Order-Revealing Encryption schemes
- Cross-column correlation
- Mitigation by inserting fake data to functionally alter the prior

Publications and Talks

[1] Quantifying Information Leakage of Deterministic Encryption, Mireya Jurado and Geoffrey Smith, in *Proc. CCSW'19:2019 Cloud Computing Security Workshop,* London, UK, November 2019

[2] Quantifying Information Leakage of Deterministic Encryption (lightning talk), Mireya Jurado and Geoffrey Smith, in *Encrypted Search Workshop*, Providence, RI, June 2019

Broader Impact

- **Scientific Impact**
  - Coupled the provable-security approach of modern cryptography with QIF theory to yield a novel security framework
  - Analyzed encrypted search schemes
- **Societal Impact**
  - Helped practitioners and researchers better understand security risks
- **Impact on Education and Outreach**
  - Florida International University is a leading Minority Institution.
  - Funded a Hispanic woman PhD student