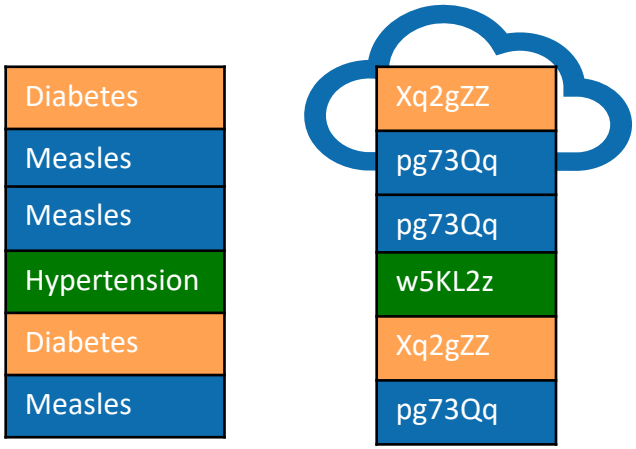
Quantifying Information Leakage in Searchable Encryption

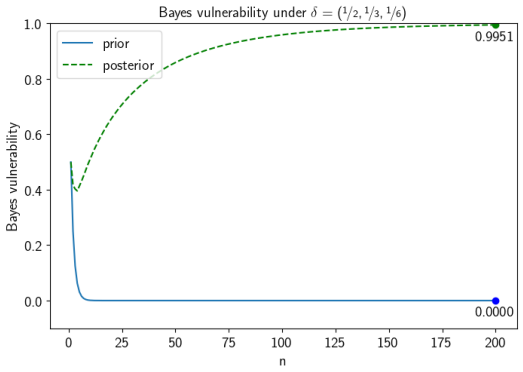


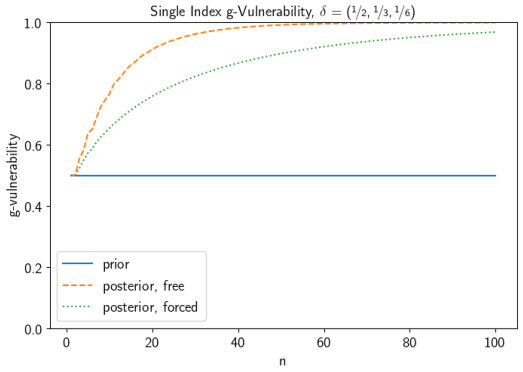
Challenge:

- Want to store sensitive data in the cloud
- *Searchable encryption* (e.g. deterministic encryption, order-revealing encryption) allows efficient search
- But what information is thereby leaked?

Solution:

- Analyze leakage using the theory of *Quantitative Information Flow (QIF)*
- Different gain functions model different operational scenarios
- *Bayes vulnerability*: adversary wants to guess entire column in one try
- *Single-index vulnerability*: adversary wants to guess some patient's disease





EAGER: Collaborative: CNS-1749014
PI: Geoffrey Smith

FIU Engineering & Computing
School of Computing & Information Sciences

Scientific Impact:

- Couple provable security of modern cryptography with information-theoretic QIF
- Quantitative assessment of security risks due to searchable encryption
- Guidance about when searchable encryption is secure

Broader Impact:

- Help practitioners and researchers better understand security risks
- Florida International University is a leading Minority Institution.

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

The Science of Quantitative Information Flow, Alvim, Chatzikokolakis, McIver, Morgan, Palamidessi, and Smith (Springer 2019)