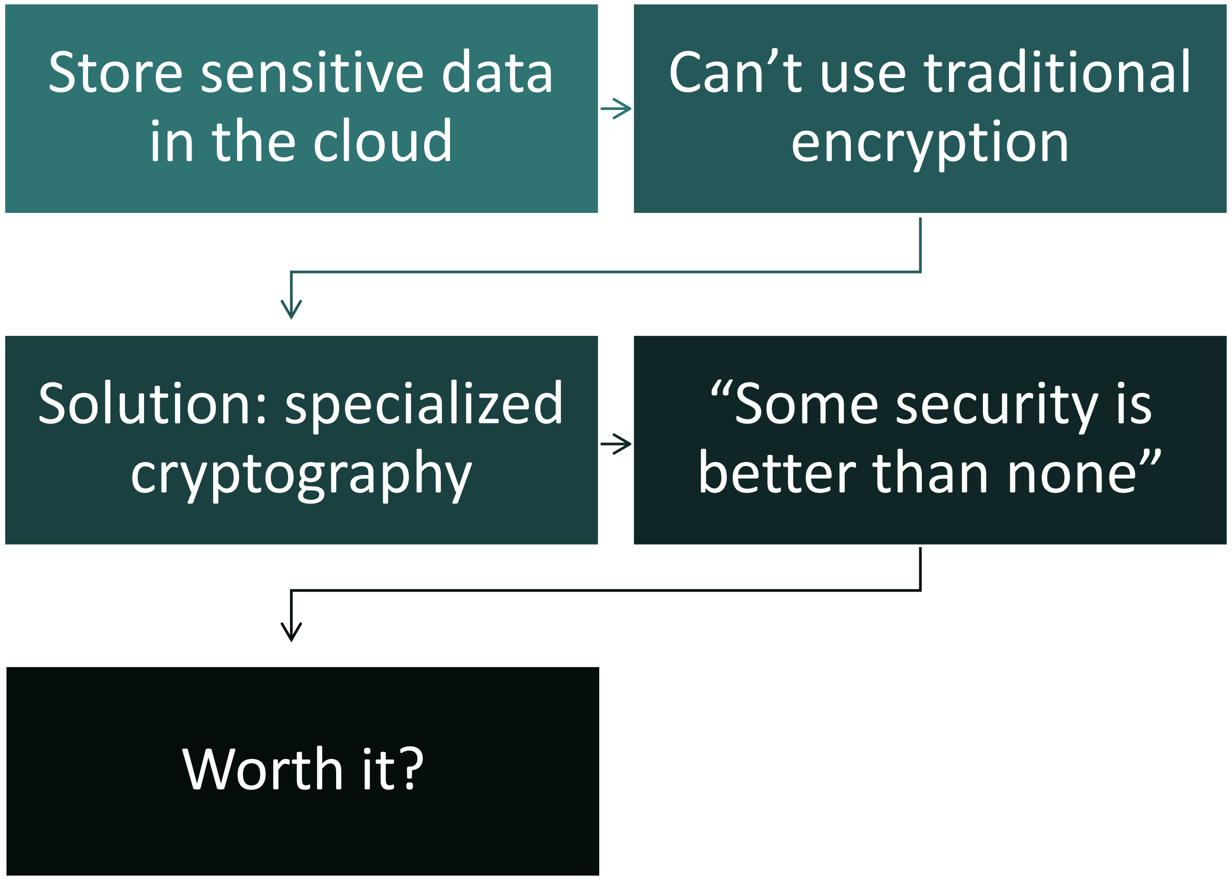
A Formal Information-Theoretic Leakage Analysis of

Order-Revealing Encryption

Mireya Jurado, Catuscia Palamidessi, Geoffrey Smith
34th IEEE Computer Security Foundations Symposium
June 24, 2021

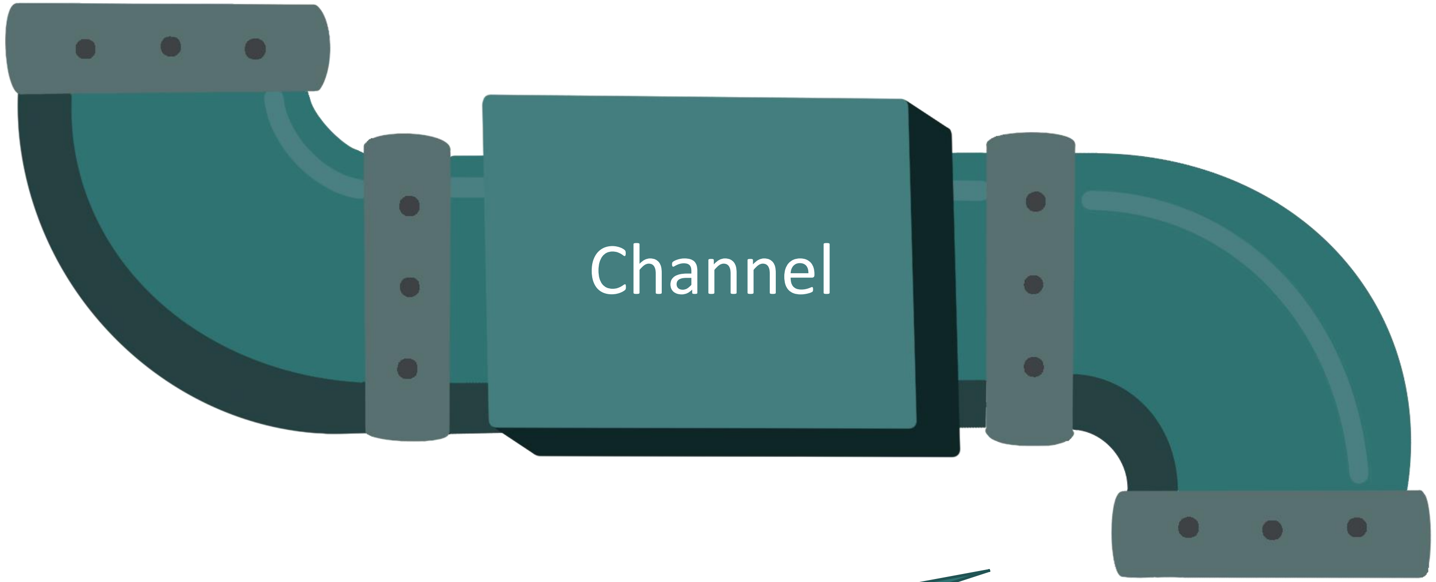
Motivation


Store sensitive data in the cloud
Can’t use traditional encryption
Solution: specialized cryptography
“Some security is better than none”
Worth it?

Quantitative Information Flow (QIF)

Secret Input X

Prior vulnerability: Given only probability distribution on secrets π



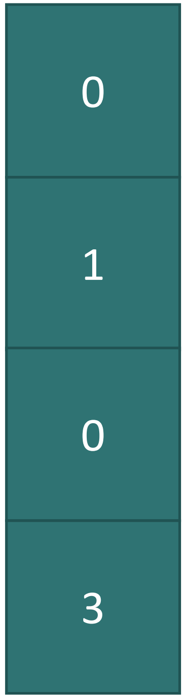
Observable Output Y

Leakage: The difference

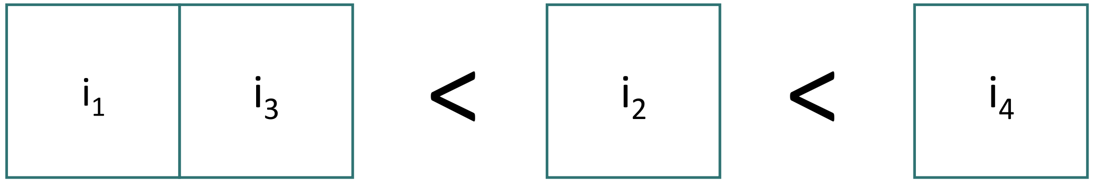
Posterior vulnerability: Given π **and** output Y

Ideal Order-Revealing Encryption (ORE)

Secret: plaintext column

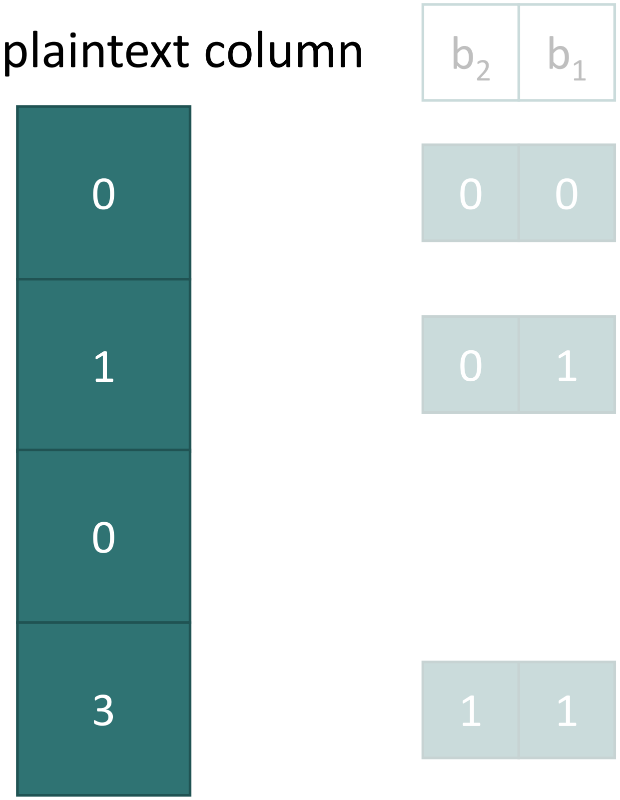


Observable: ordered partition of blocks

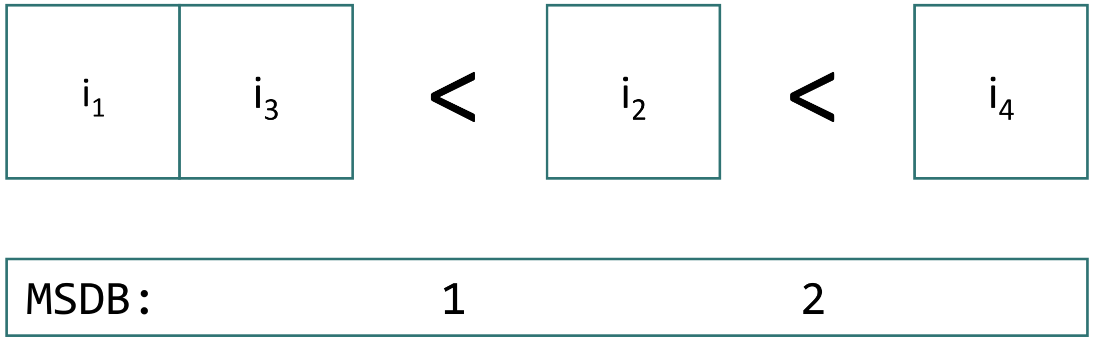


CLWW ORE

Secret: plaintext column

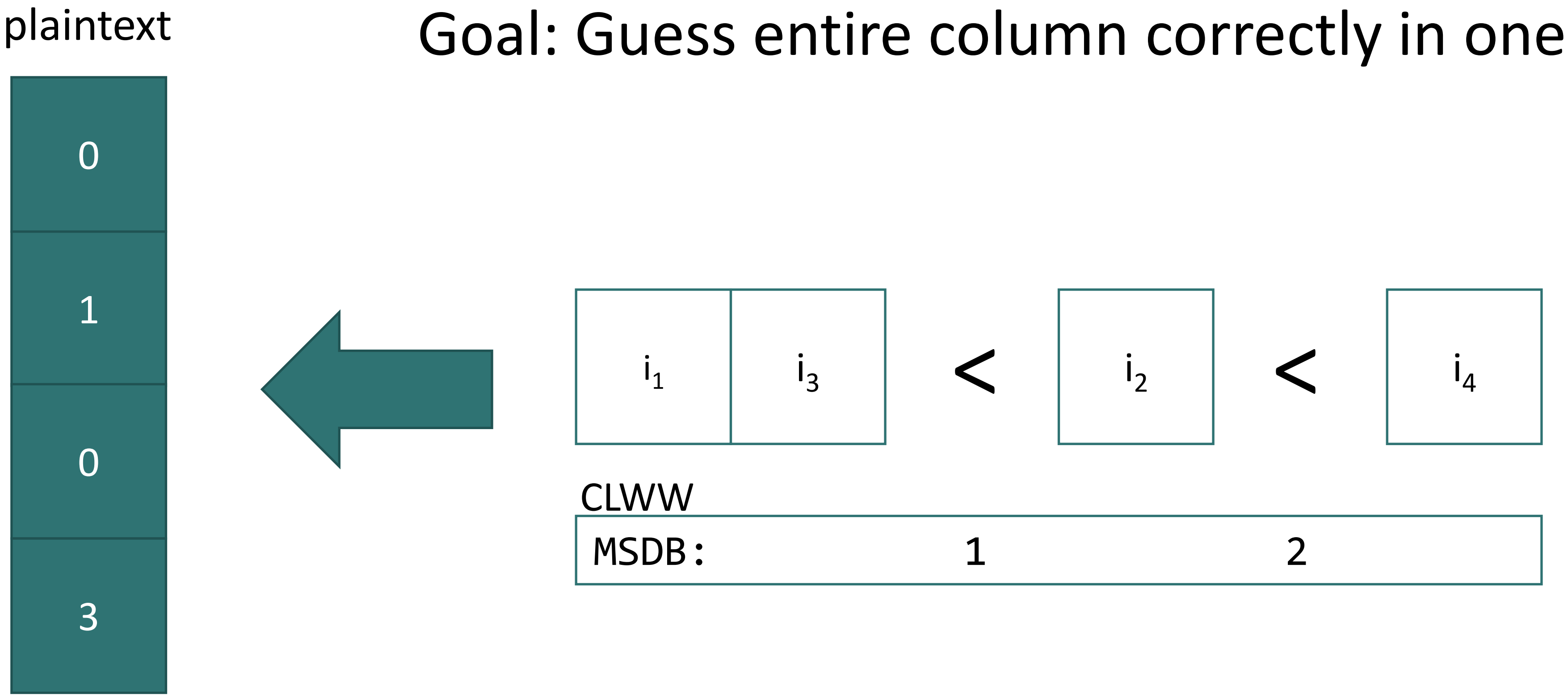


Observable: ordered partition of blocks
+ index of most significant differing bit (MSDB)

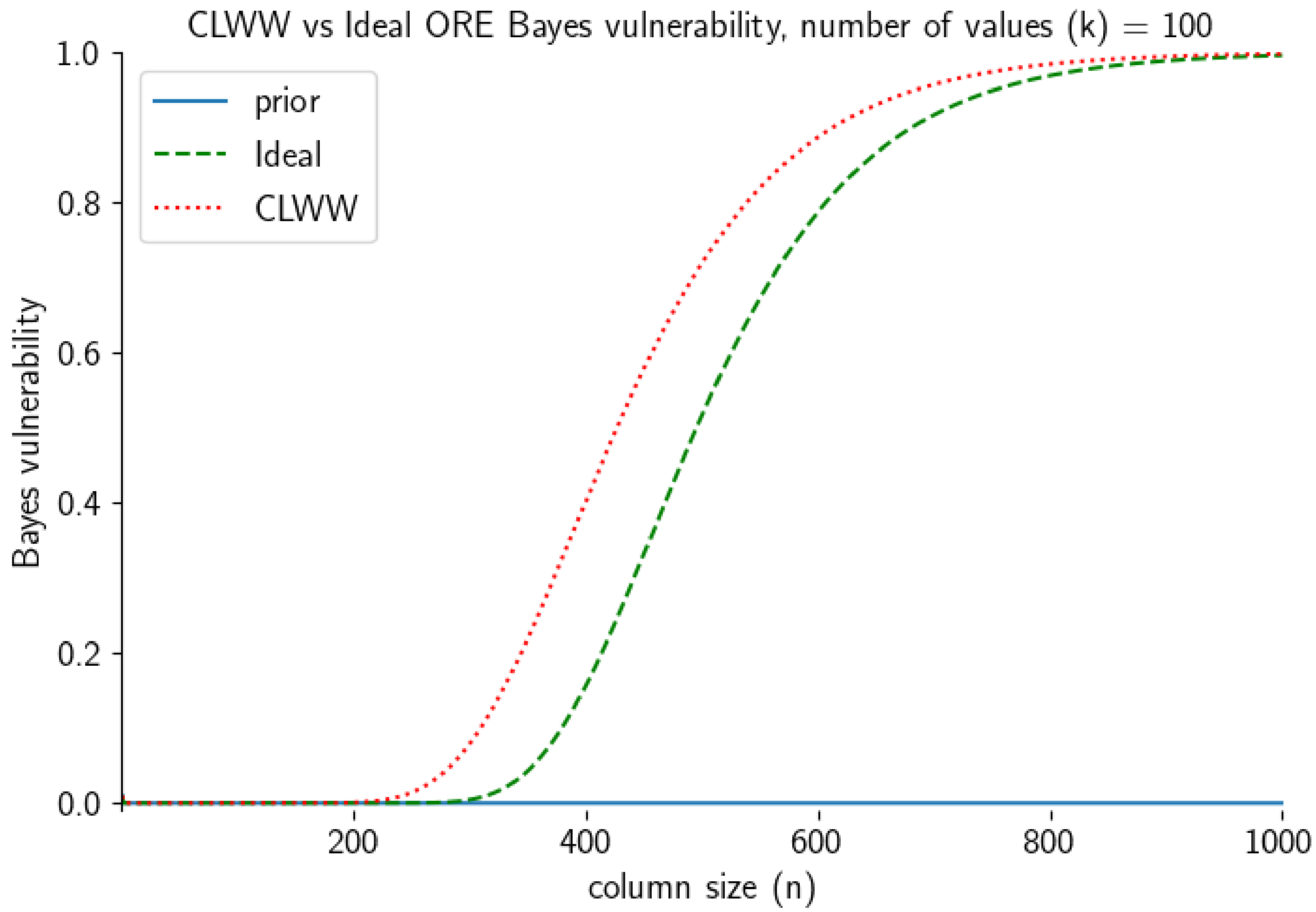


Bayes Vulnerability

Goal: Guess entire column correctly in one try

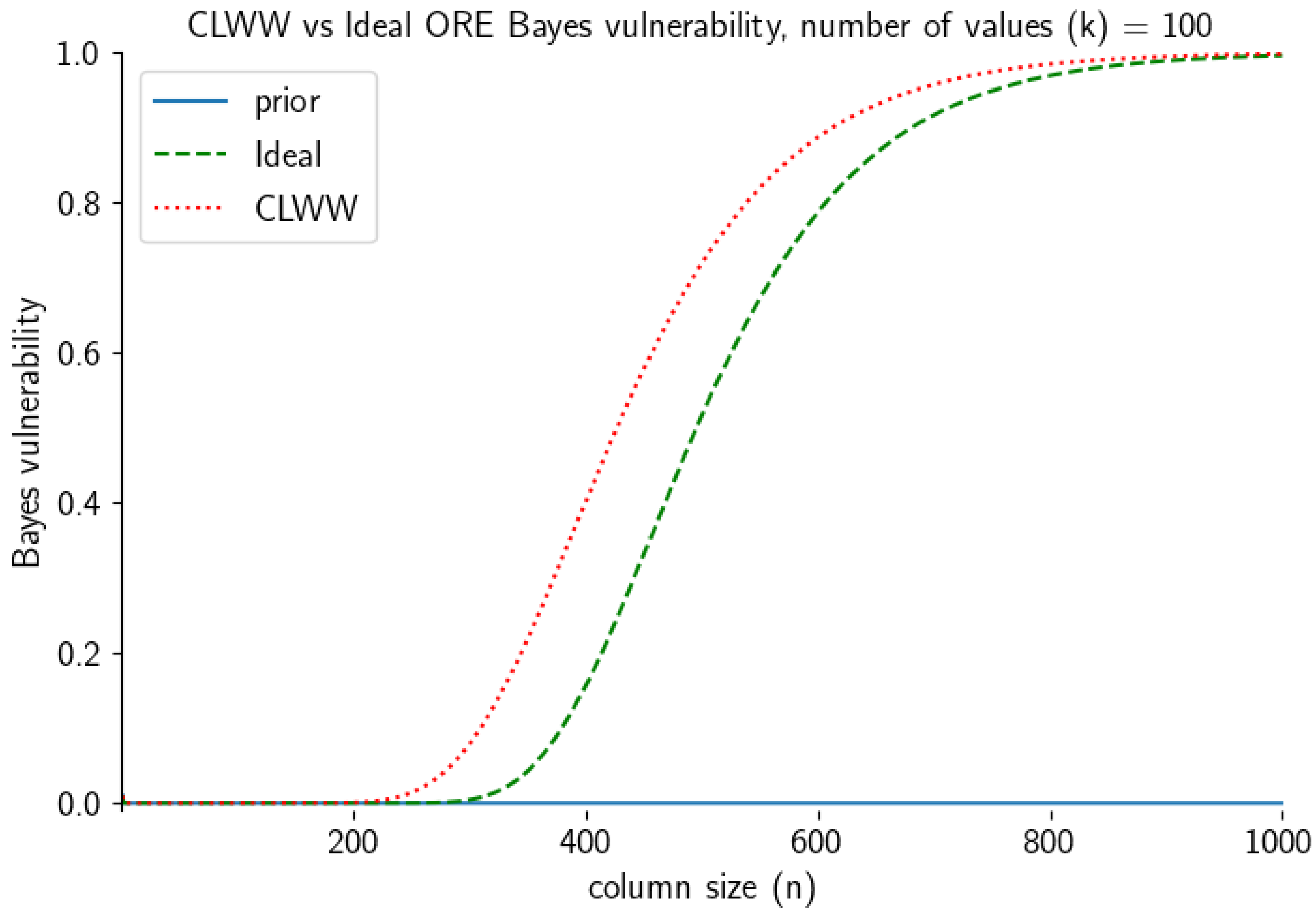


Bayes Vulnerability



- As database grows, greater chance all values appear
- Easier to order values and map to plaintexts

Bayes Vulnerability

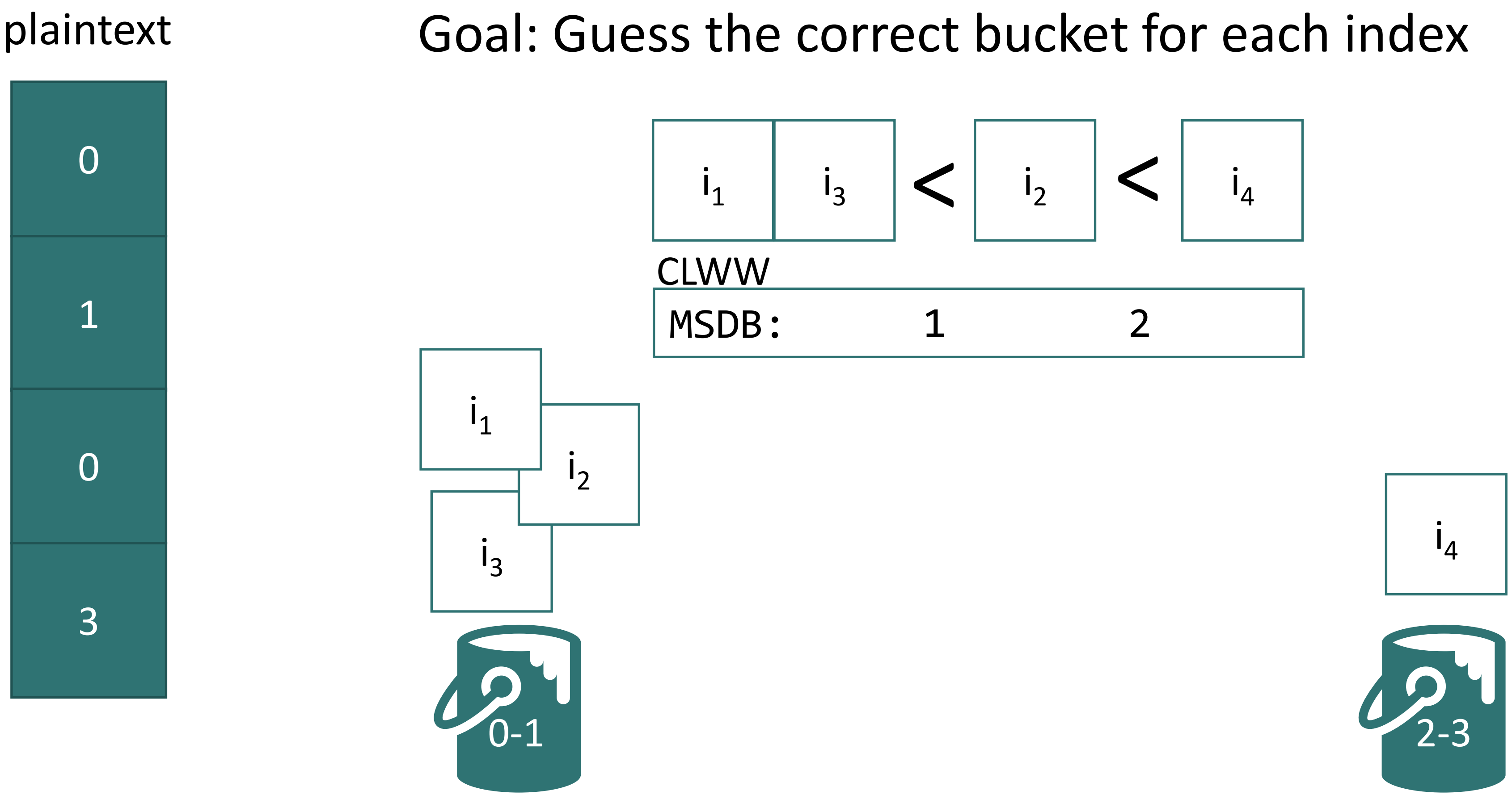


- If the column is sparse k ≥ n, posterior Bayes vulnerability of Ideal ORE is very small
- Theorem 5:

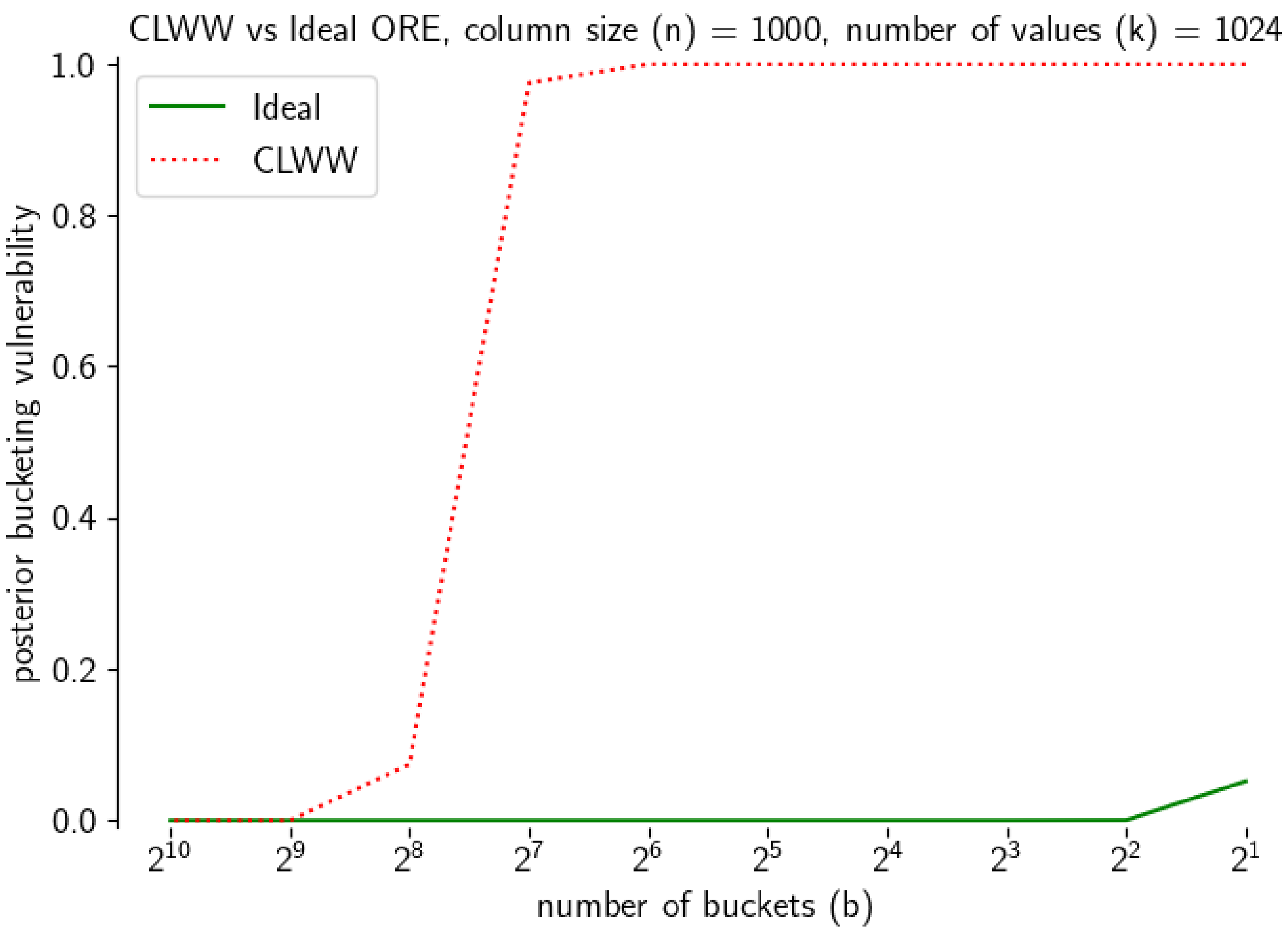
  If $k \geq n \geq 1$, then:

  $$\text{Bayes}_{I}(n, k) \leq \left(\frac{3}{4}\right)^{n-1} \times \left(\frac{n}{k}\right)^{n}$$

Bucketing Vulnerability



Bucketing Vulnerability



- Because a bucketing adversary is so natural, CLWW is fundamentally insecure

Mitigation

Append randomly chosen bits prior to encrypting

Range queries: pad bounds with 0s & 1s

Transparent to the user

Improves posterior vulnerability of Ideal ORE

Contributions

- Analyzed the leakage of Ideal & CLWW ORE using novel combinatorics
- Established usage guideline for Ideal ORE under a Bayes adversary
- Showed Ideal ORE is robust under bucketing while CLWW ORE is not
- Developed a mitigation strategy for Ideal ORE