

IHOOP

Simon Oya

Florian Kerschbaum

Improved Statistical
Query Recovery against
Searchable Encryption through
Quadratic Optimization

University of Waterloo

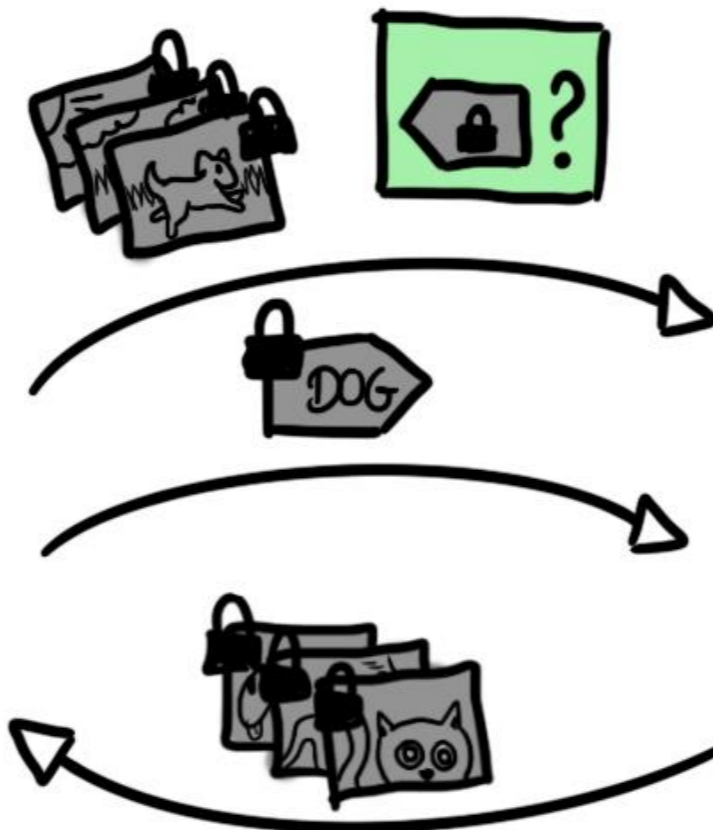
CrySP



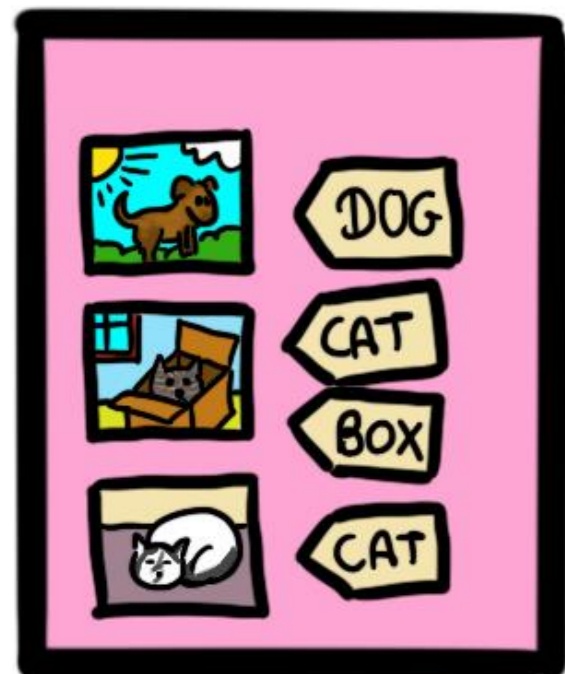
Overview: Searchable Encryption



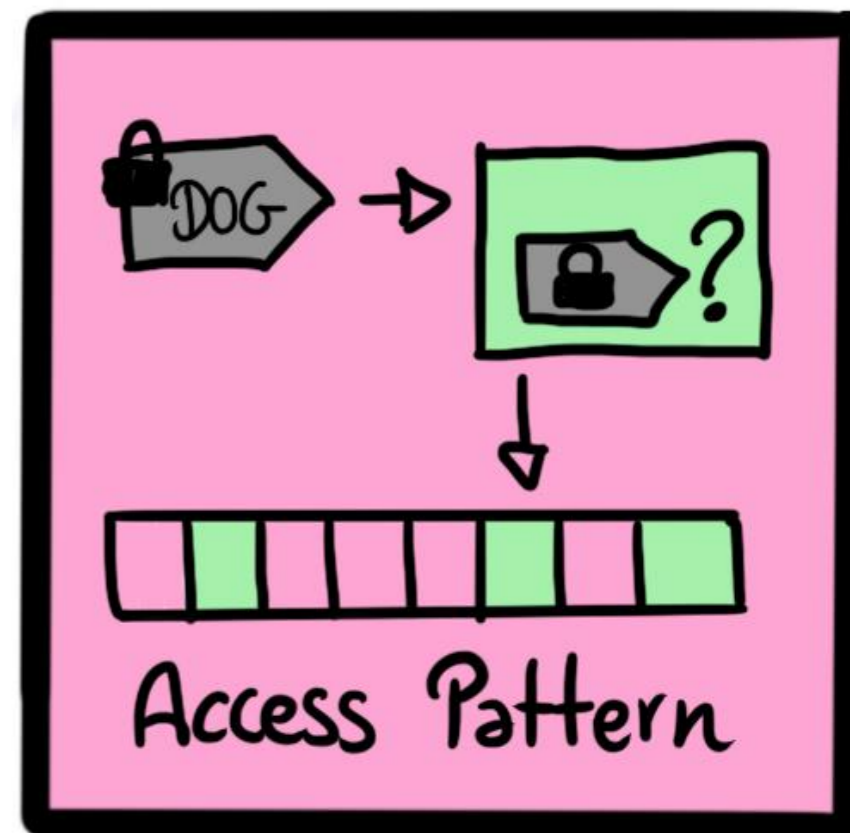
Alice



Server



Encrypted Search index

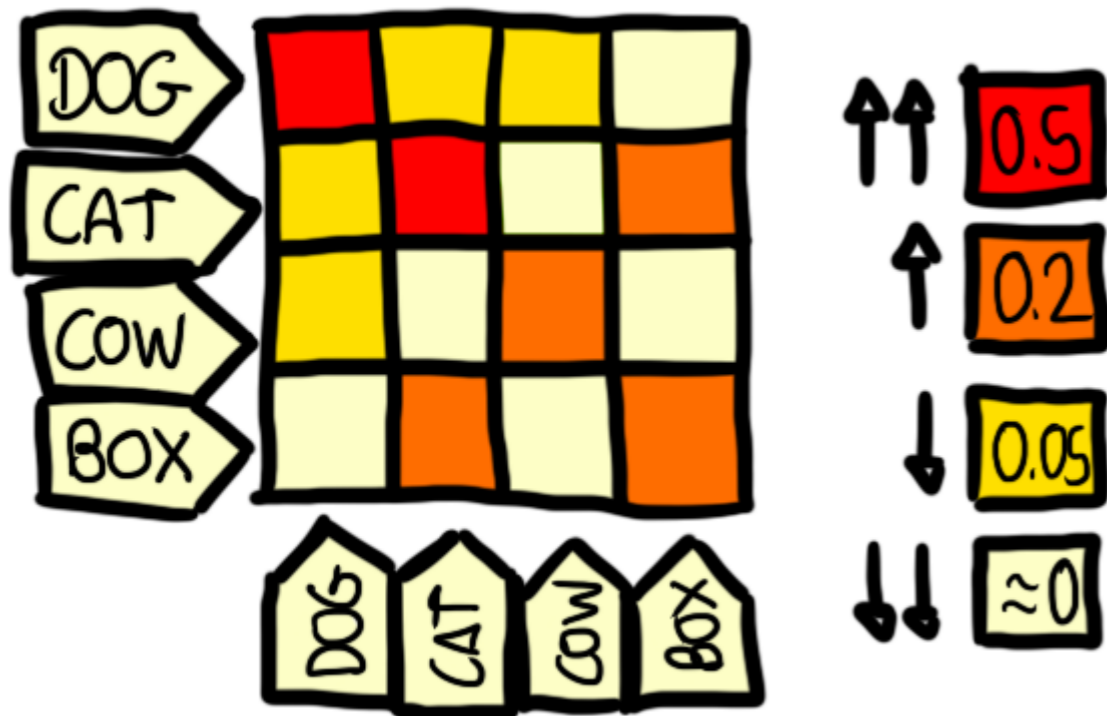


Leakage & Adversary Model

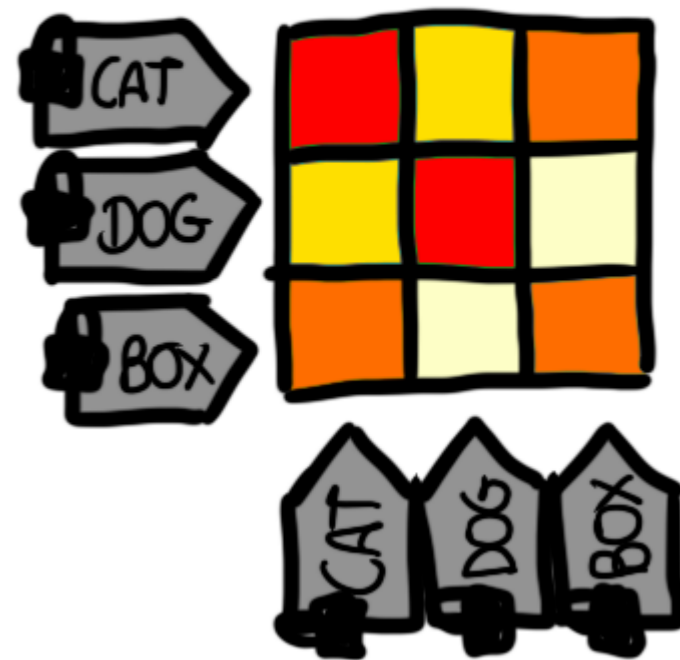
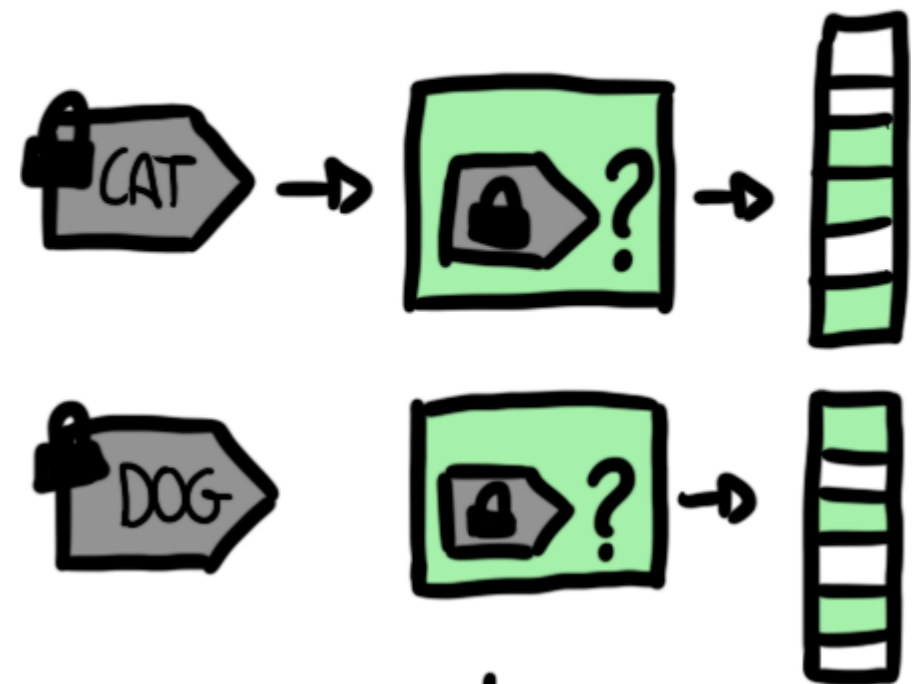
Auxiliary Information



↓ Volume
co-occurrence



Observations

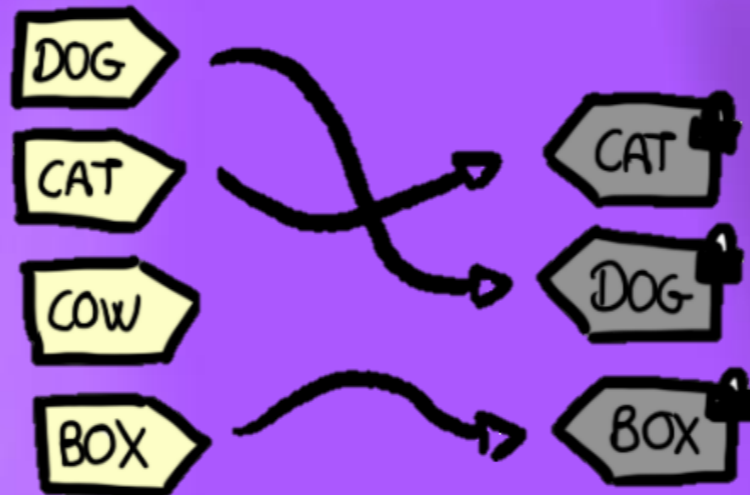
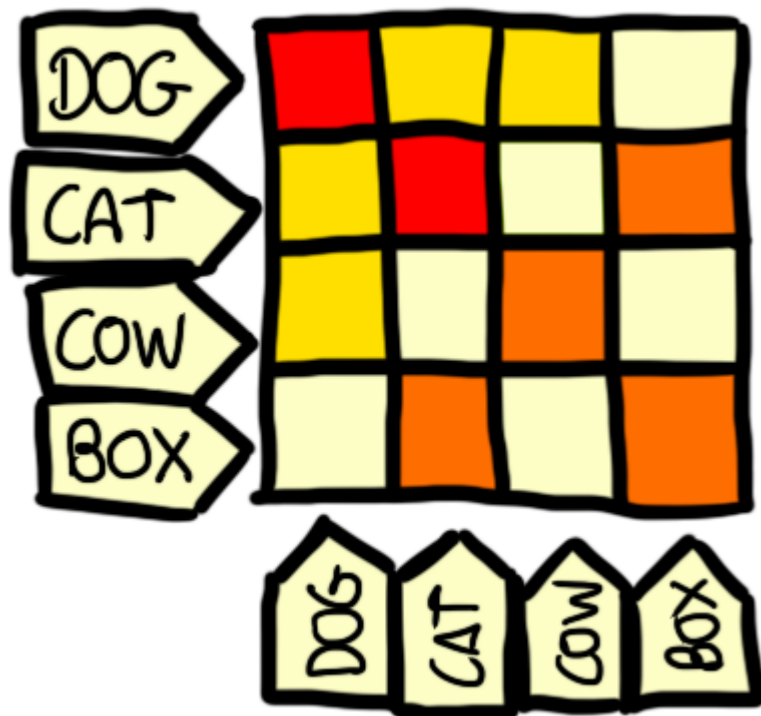


Leakage & Adversarial Model

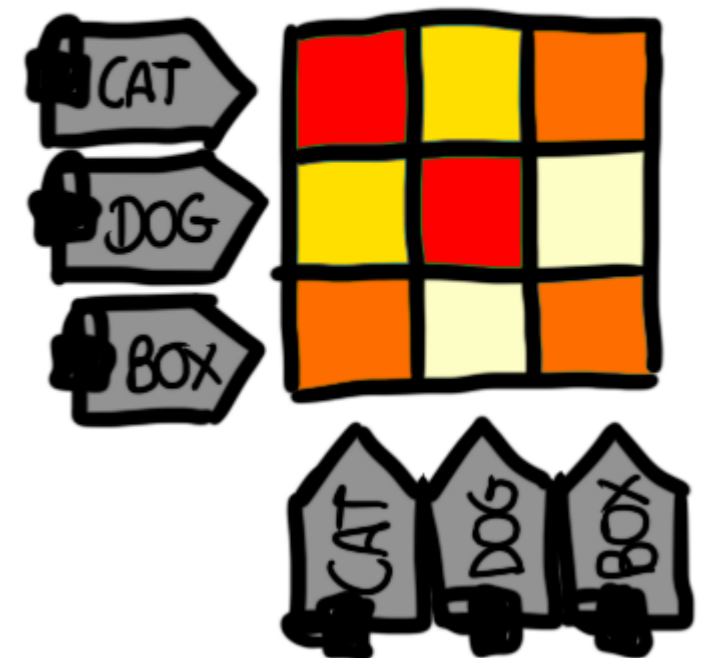
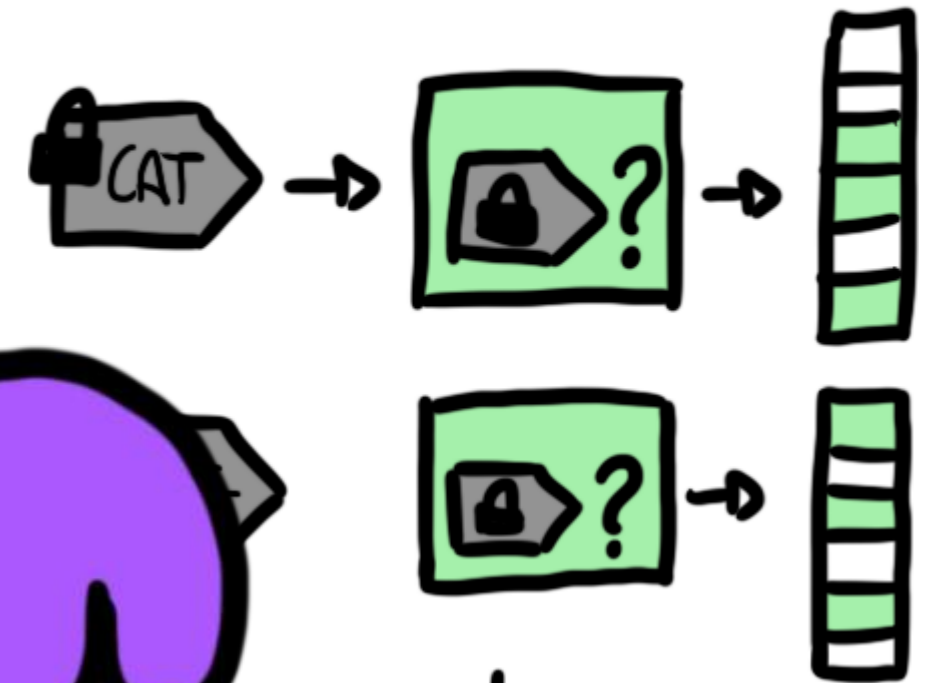
Auxiliary Information



↓ Volume
co-occurrence

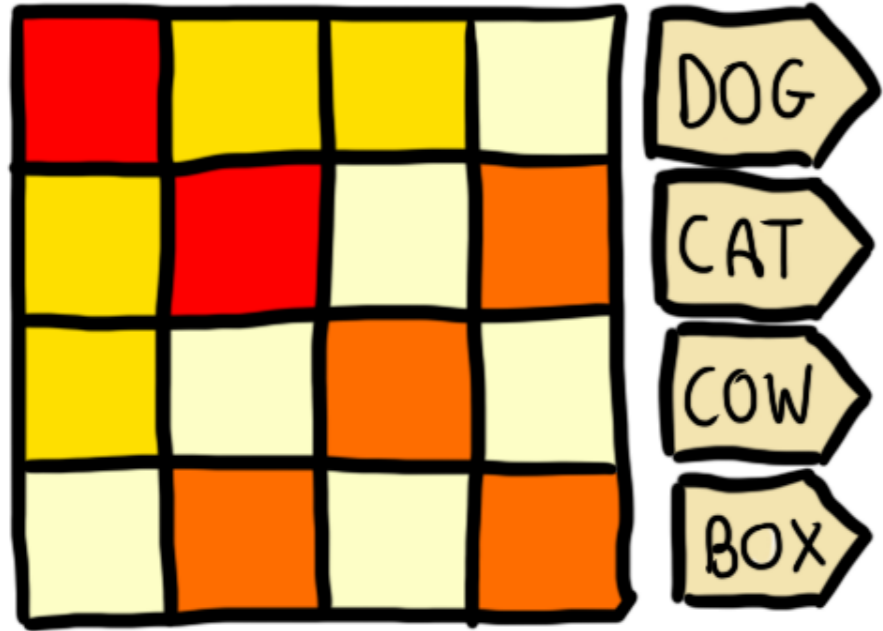


Observations

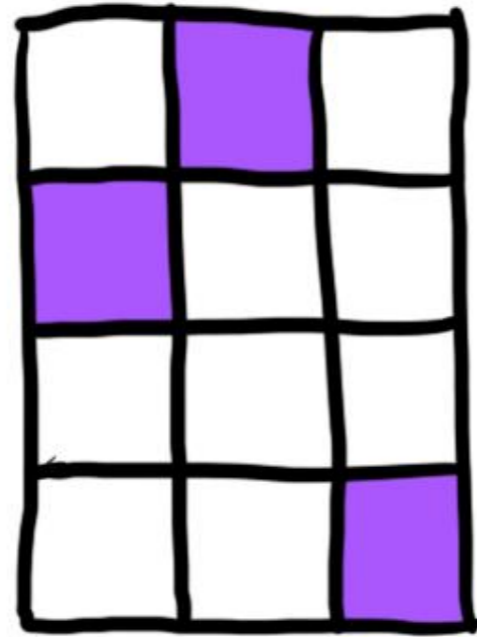


Quadratic Assignment Problem (QAP)

$\tilde{V} (n \times n)$ (AUX)



$P (n \times m)$



$$P = \underset{P \in \mathcal{P}}{\operatorname{argmin}} \sum_{\substack{i \rightarrow j \\ \text{DOG}}} \sum_{\substack{i \rightarrow j \\ \text{CAT}}} C_{ij} \cdot P_{ij} \cdot P_{ij}$$



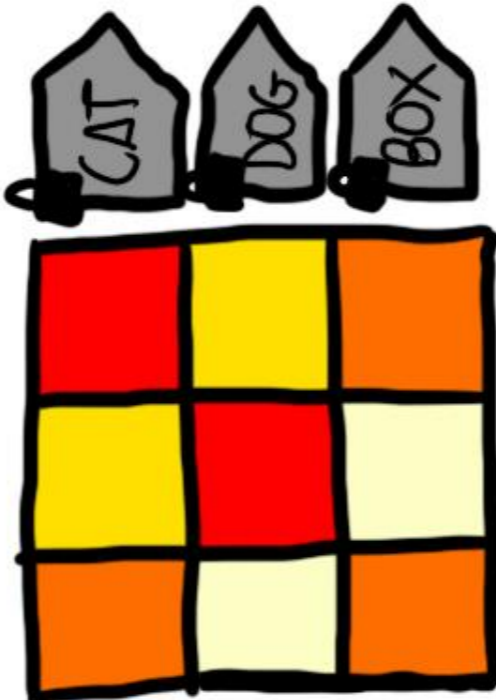
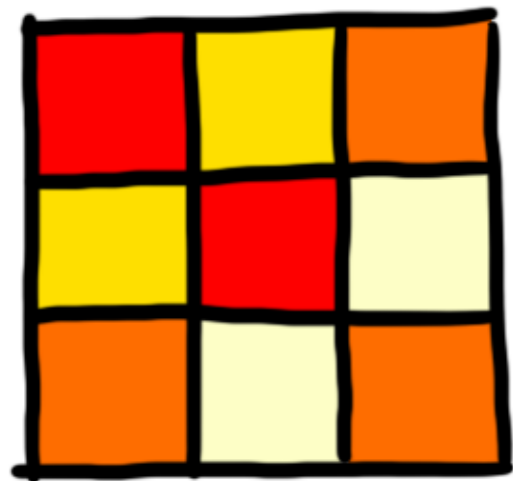
Examples

IKK [1]: $P = \underset{P \in \mathcal{P}}{\operatorname{argmin}} \| \tilde{V} - PVP^T \|_2 \rightarrow \text{Annealing}$

graphm [2]: $P = \underset{P \in \mathcal{P}}{\operatorname{argmin}} \| \tilde{V} - PVP^T \|_2^2 - \operatorname{tr}(CP)$

↳ Convex-concave rel.

$$P^T \tilde{V} P$$



(OBS)

$V (m \times m)$

[1] Islam et al. *Access pattern disclosure on searchable encryption: Ramification, attack and mitigation*. NDSS 2012.

[2] Pouliot and Wright. *The shadow nemesis: Inference attacks on efficiently deployable, efficiently searchable encryption*. CCS 2016

Linear Assignment Problem (LAP)

SAP [3]

$\tilde{V}(n \times n)$

$P(n \times m)$

Red	Yellow	Yellow	Light Yellow
Yellow	Red	Light Yellow	Orange
Yellow	Light Yellow	Orange	Light Yellow
Light Yellow	Orange	Light Yellow	Orange

DOG
CAT
COW
BOX

Purple	White	White
White	Purple	White
White	White	White
White	White	Purple

$$P = \operatorname{argmin}_{P \in \mathcal{P}} \sum_{i \rightarrow j} d_{ij} \cdot P_{ij}$$

$$O(n \cdot m + m^2 \cdot \log m)$$



0.5	0.51	0.18	0.2
-----	------	------	-----

CAT DOG BOX

0.01	0.02	0.31	0.29
0.01	0	0.33	0.31
0.3	0.31	0.02	0

0.49
0.51
0.2

Red	Yellow	Orange
Yellow	Red	Light Yellow
Orange	Light Yellow	Orange

$V(m \times m)$



But lots of wasted information

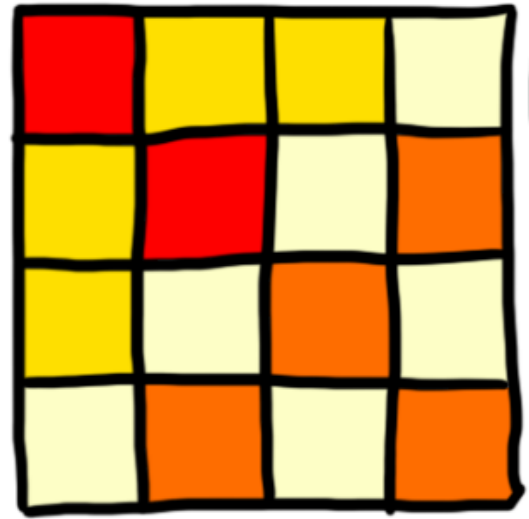


[3] Oya and Kerschbaum. *Hiding the access pattern is not enough: Exploiting search pattern leakage in searchable encryption*. USENIX 2021

Hungarian algorithm

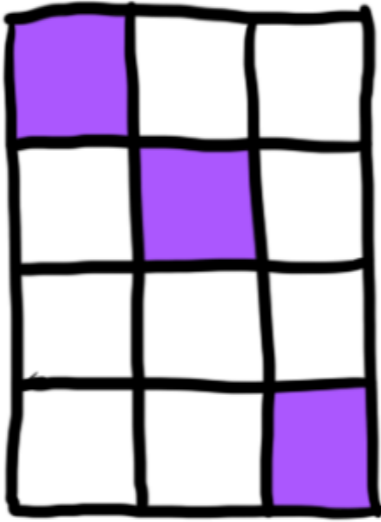
IHOP: Iteration Heuristic for (Quadratic) Optimization Problems

\tilde{V} (aux)

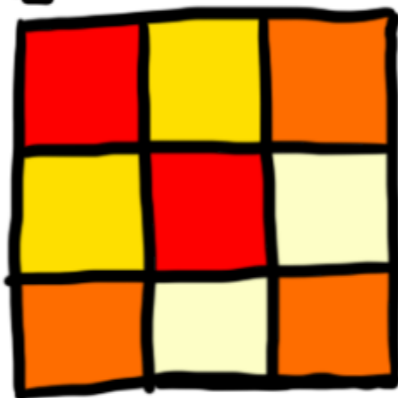


DOG
CAT
COW
BOX

P

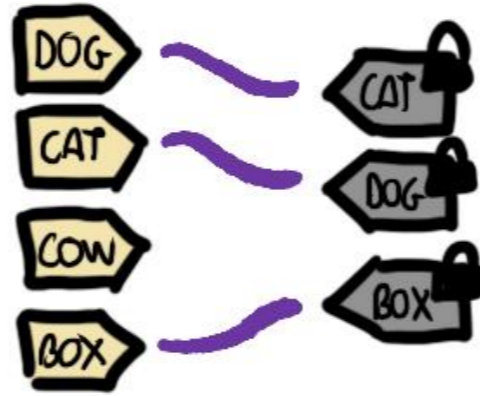


CAT
DOG
BOX



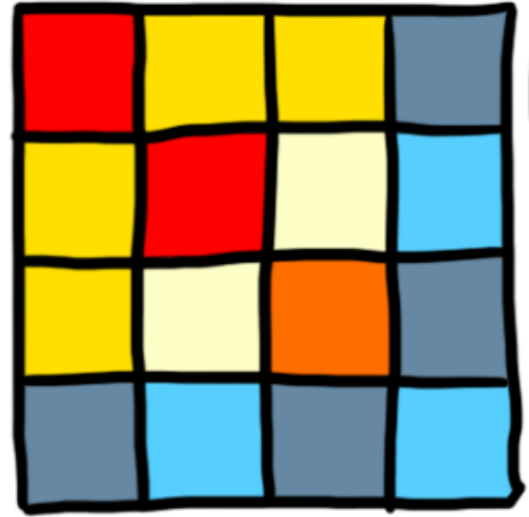
V (obs)

① Full assignment

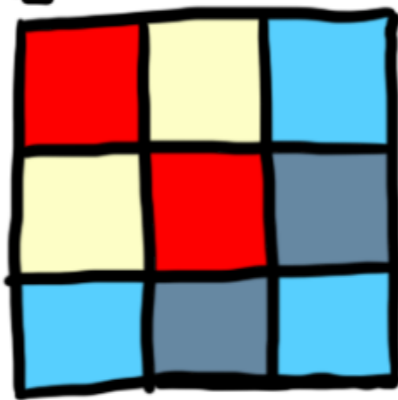
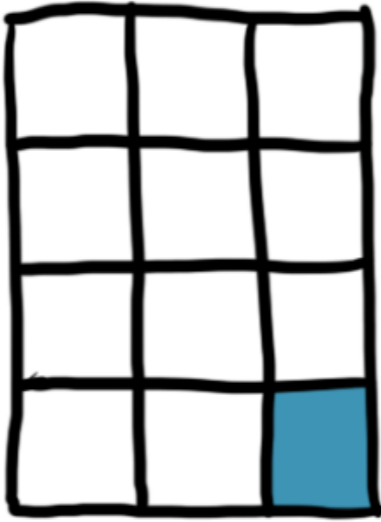


IHOP: Iteration Heuristic for (Quadratic) Optimization Problems

\tilde{V} (aux)

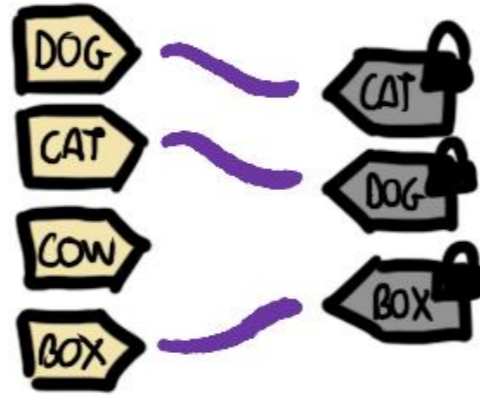


P

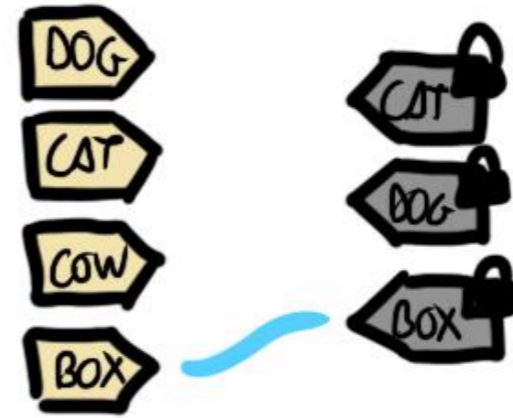


V (obs)

① Full assignment

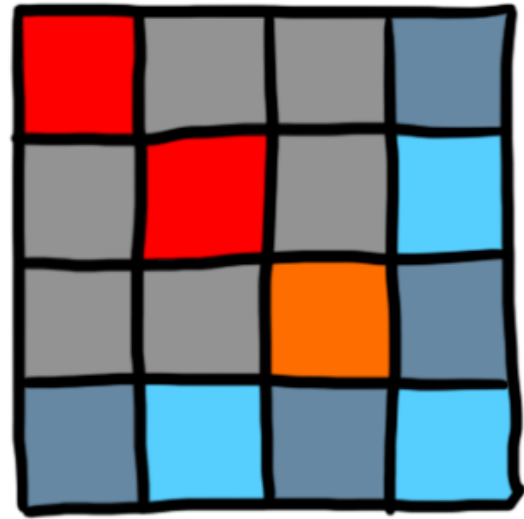


② Freeze some " ~ "

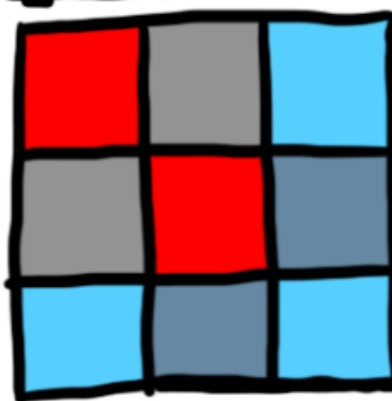
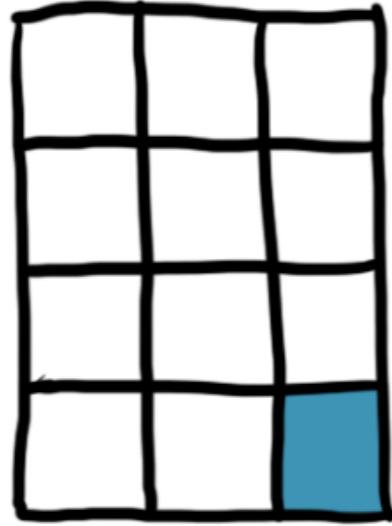


IHOP: Iteration Heuristic for (Quadratic) Optimization Problems

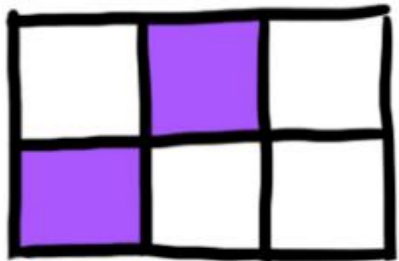
\tilde{V} (aux)



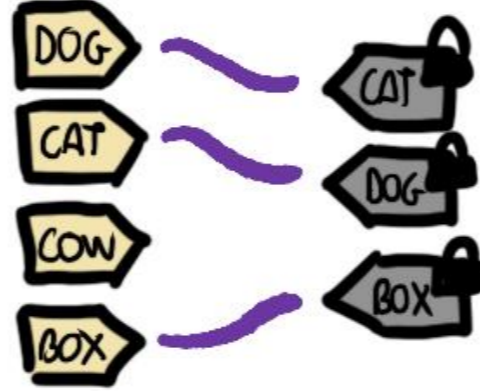
P



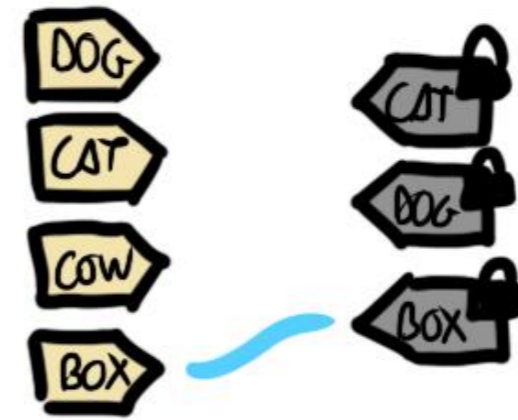
V (obs)



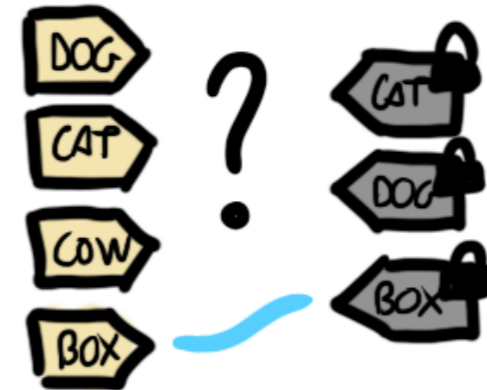
① Full assignment



② Freeze some " ~ "

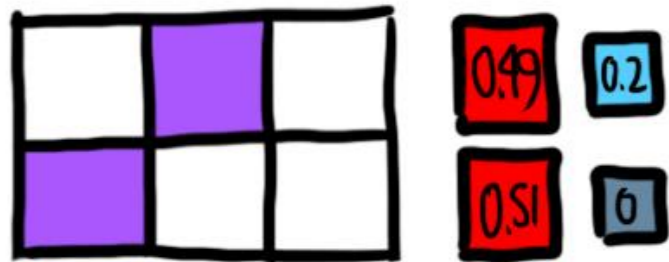
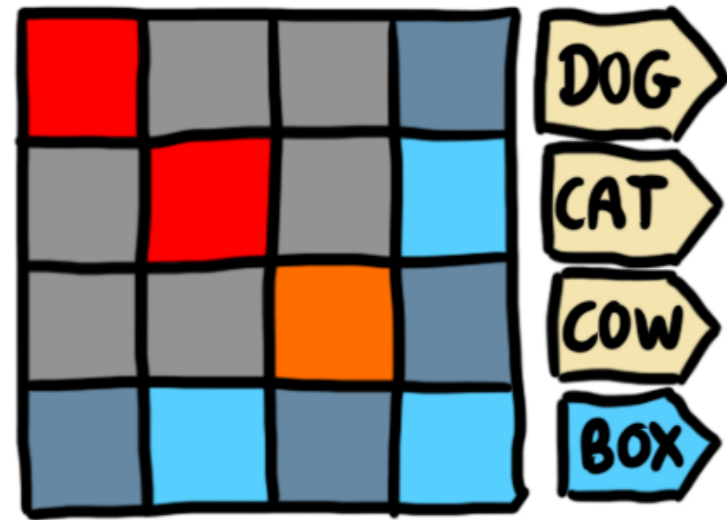


③ LAP w/ frozen

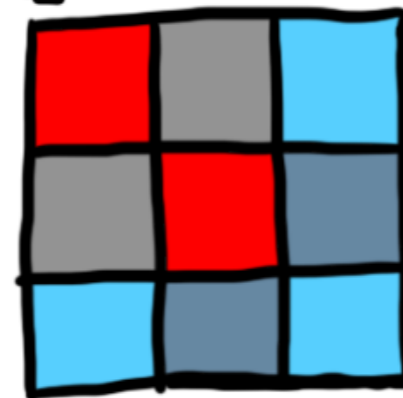
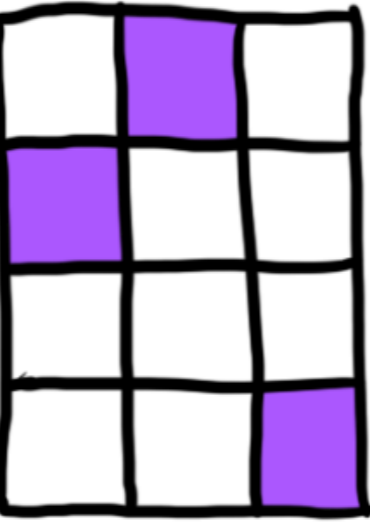


IHOP: Iteration Heuristic for (Quadratic) Optimization Problems

\tilde{V} (aux)

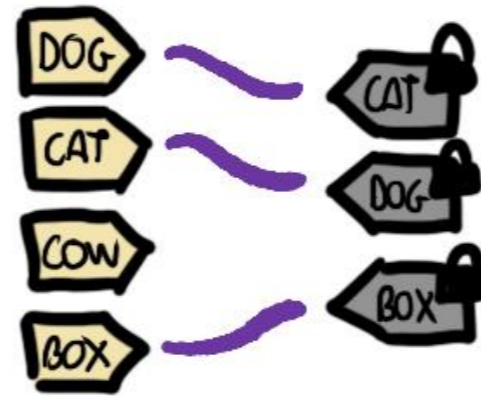


P

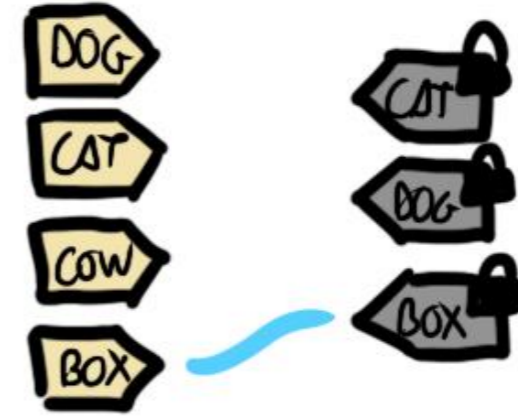


V (obs)

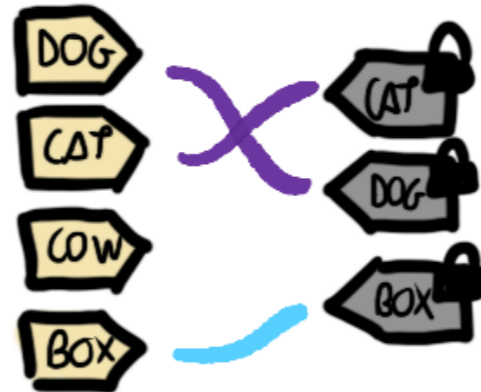
① Full assignment



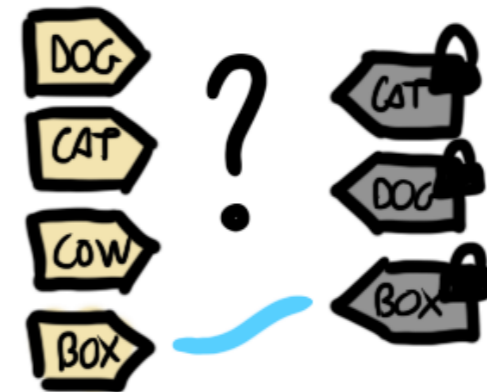
② Freeze some " ~ "



④ Solve LAP

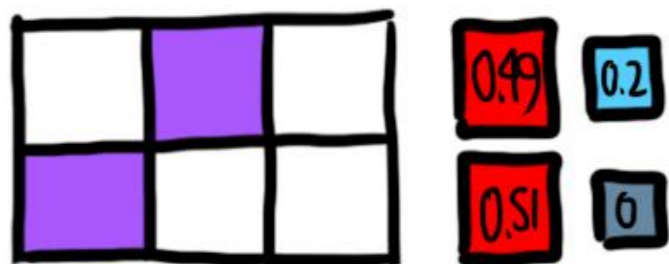
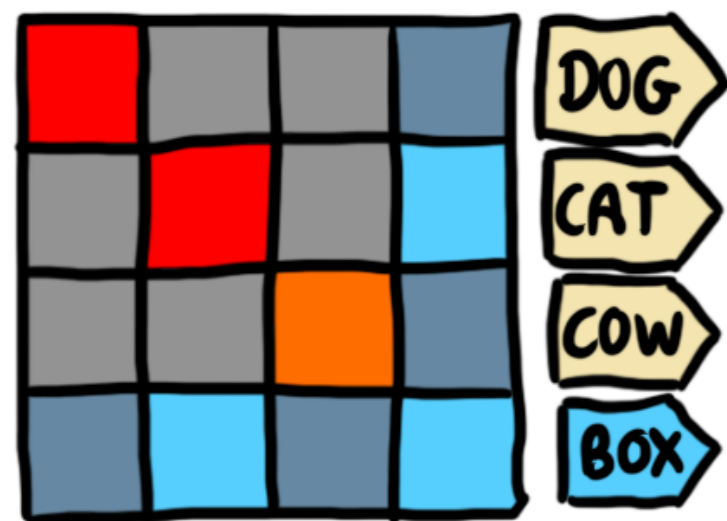


③ LAP w/ frozen

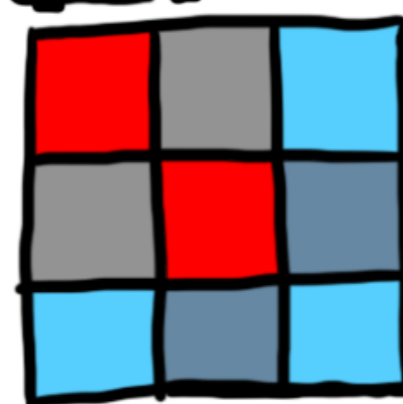
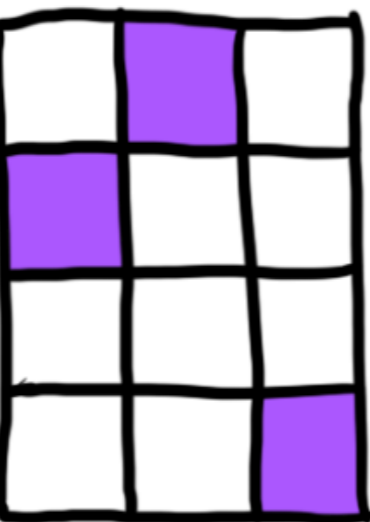


IHOP: Iteration Heuristic for (Quadratic) Optimization Problems

\tilde{V} (aux)

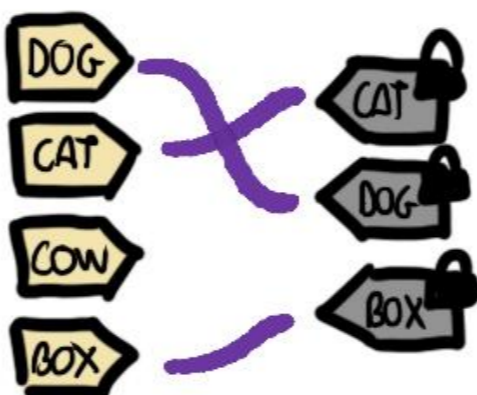


P

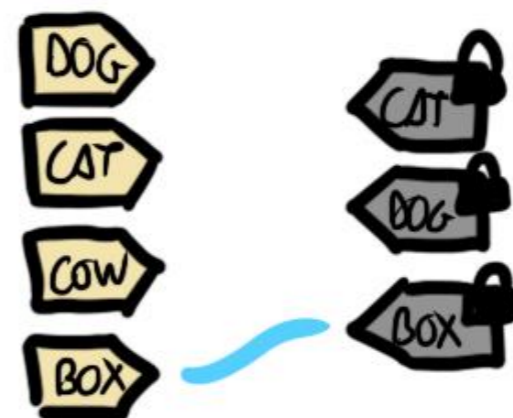


V (obs)

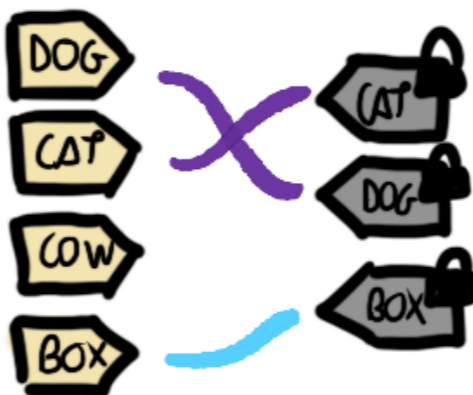
① Full assignment



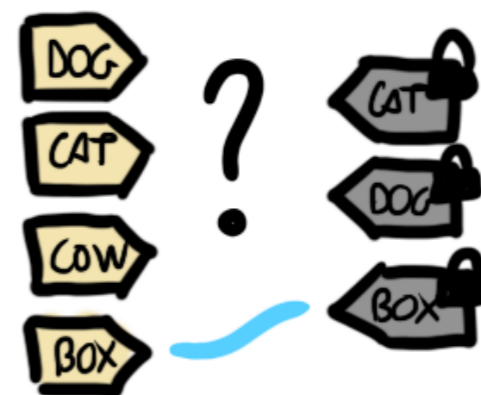
② Freeze some " ~ "



④ Solve LAP

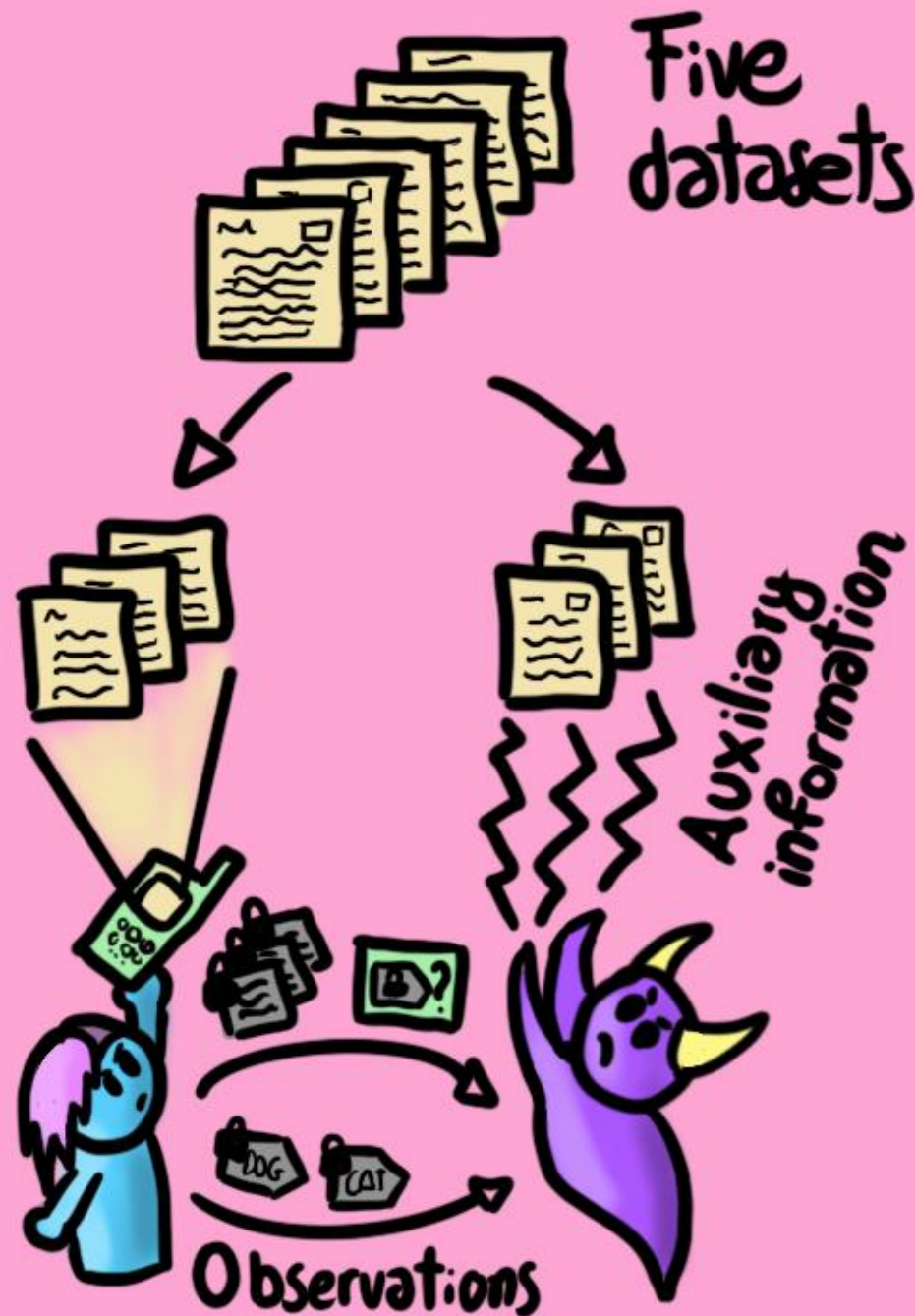


③ LAP w/ frozen

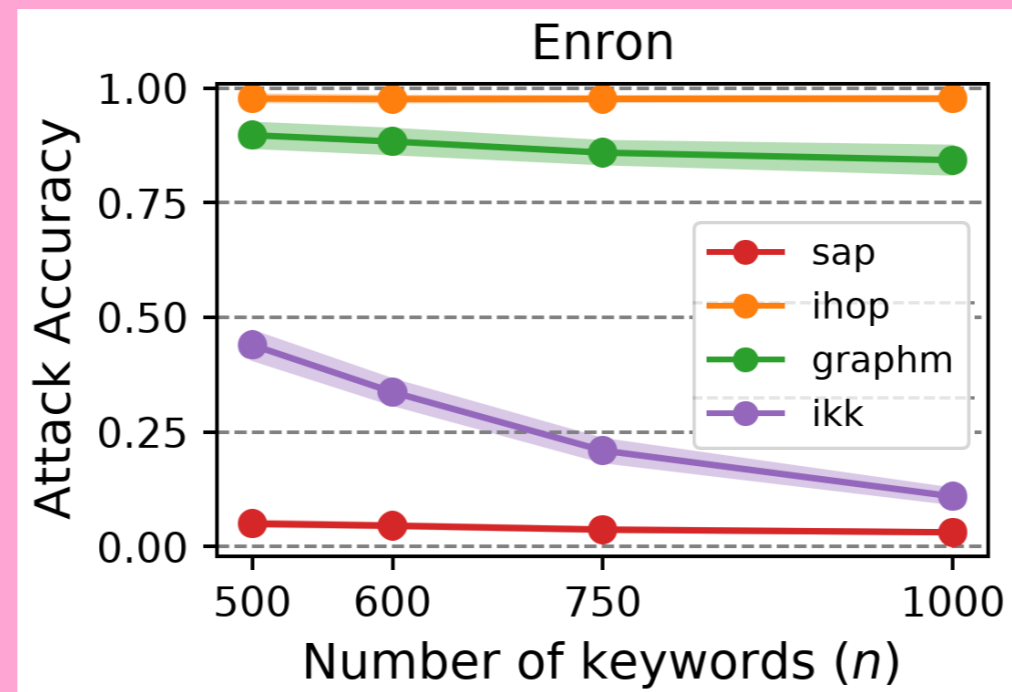
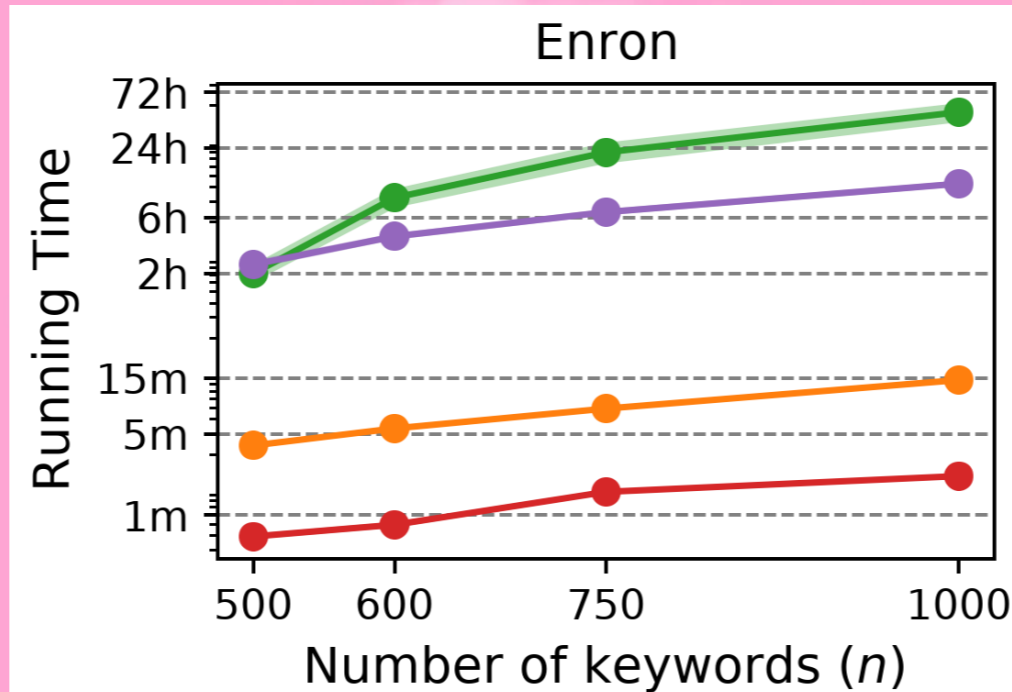


Some experiments

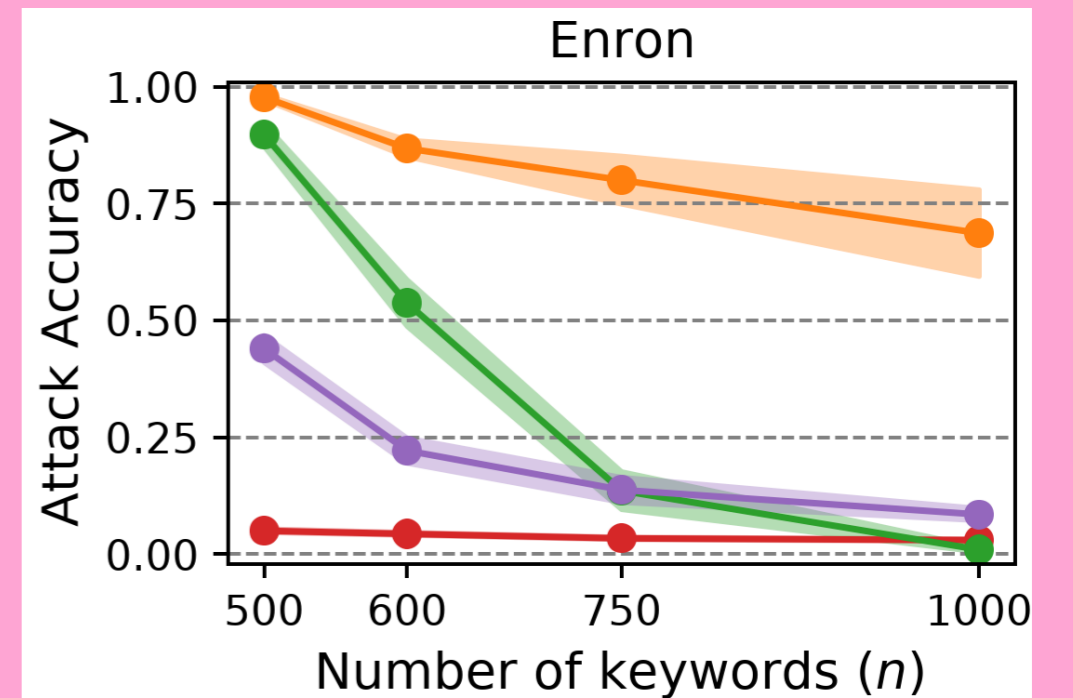
Setup



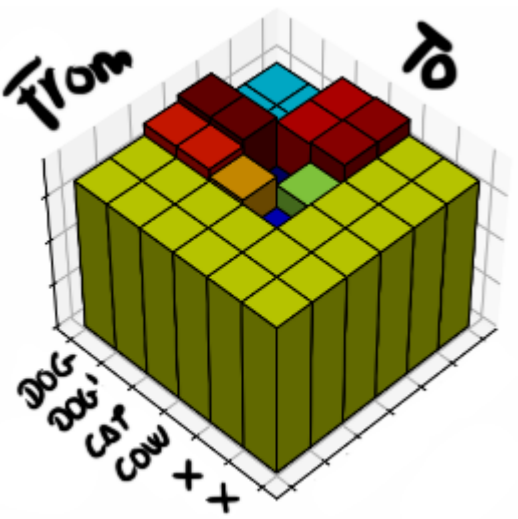
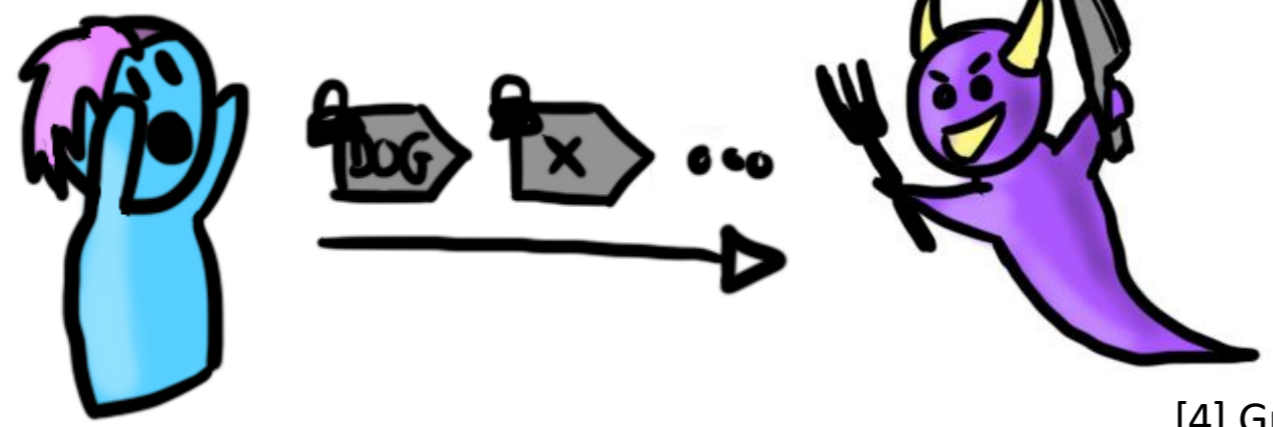
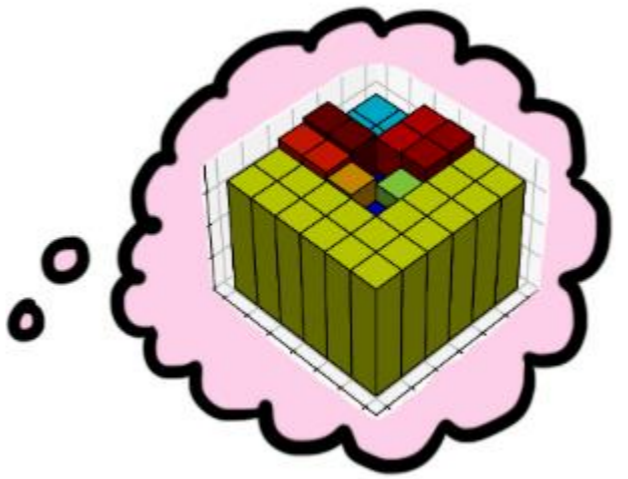
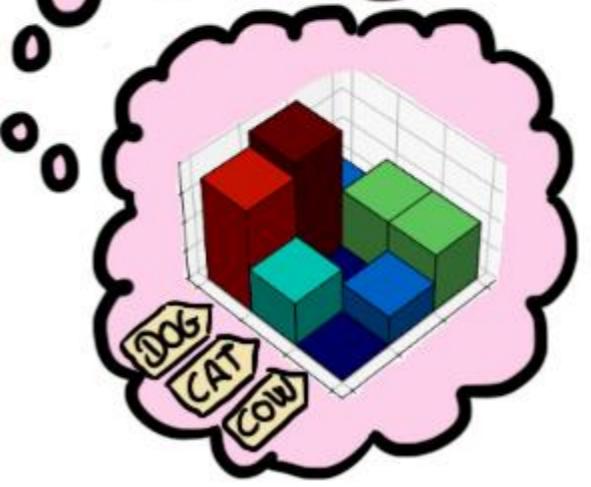
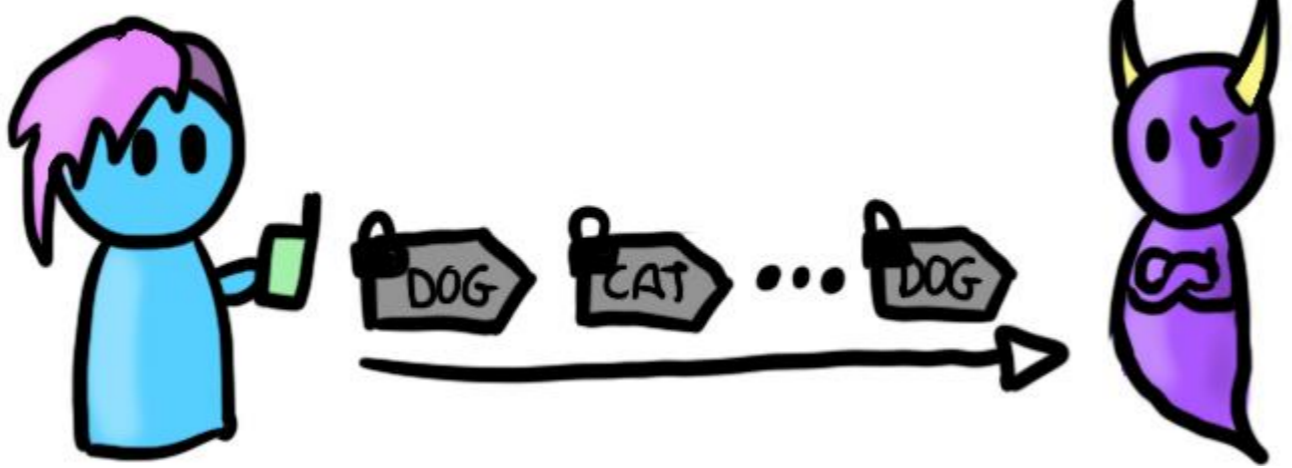
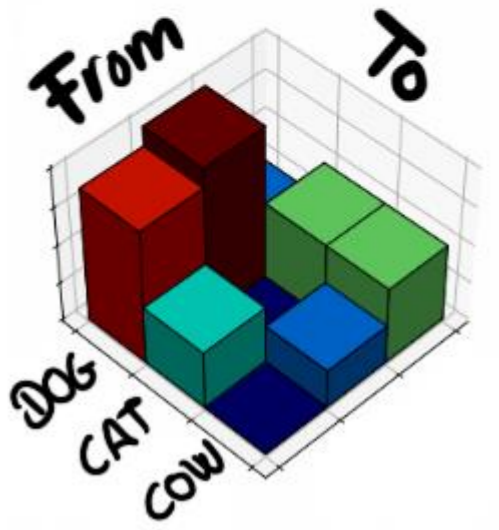
Attacks vs. # =



Attacks vs. # ≠



IHOP vs. Pancake 🥞 (very briefly)

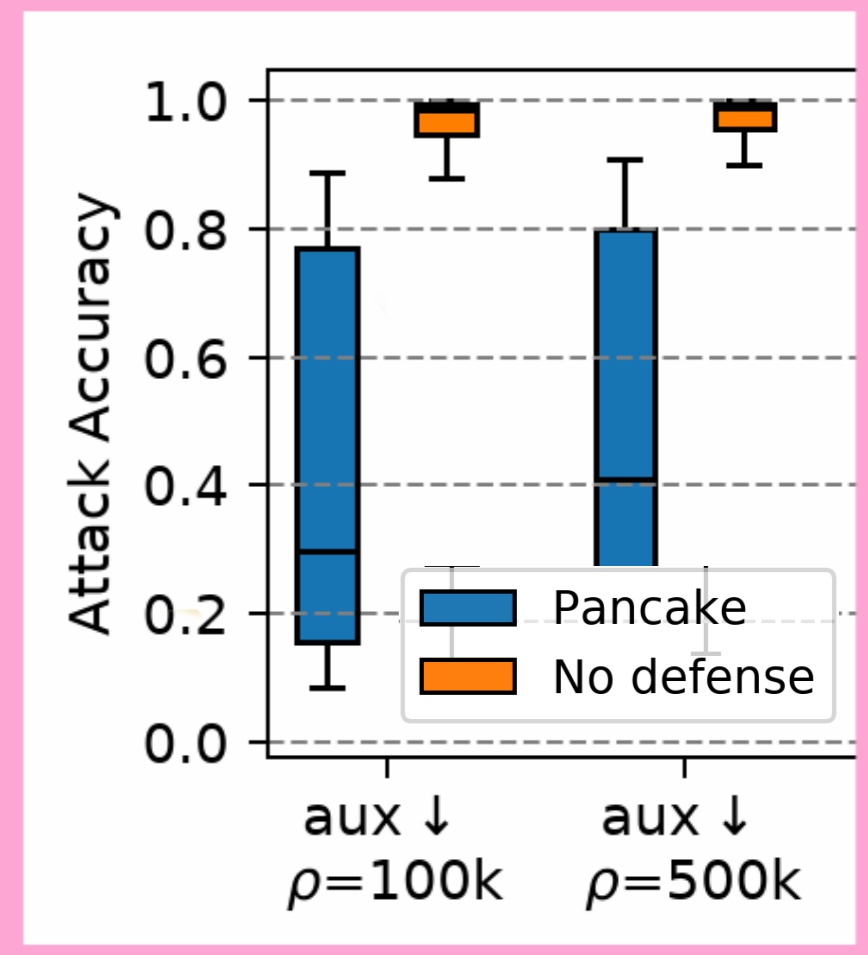


Some Results

Wikipedia Datasets

500 documents

↓
1000 replicas 🥞



I HOP

Questions?

Simon.oya@uwaterloo.ca

FASTER!

New!
Statistical Query
Recovery Attack

**MORE
ACCURATE!**

FLEXIBLE

