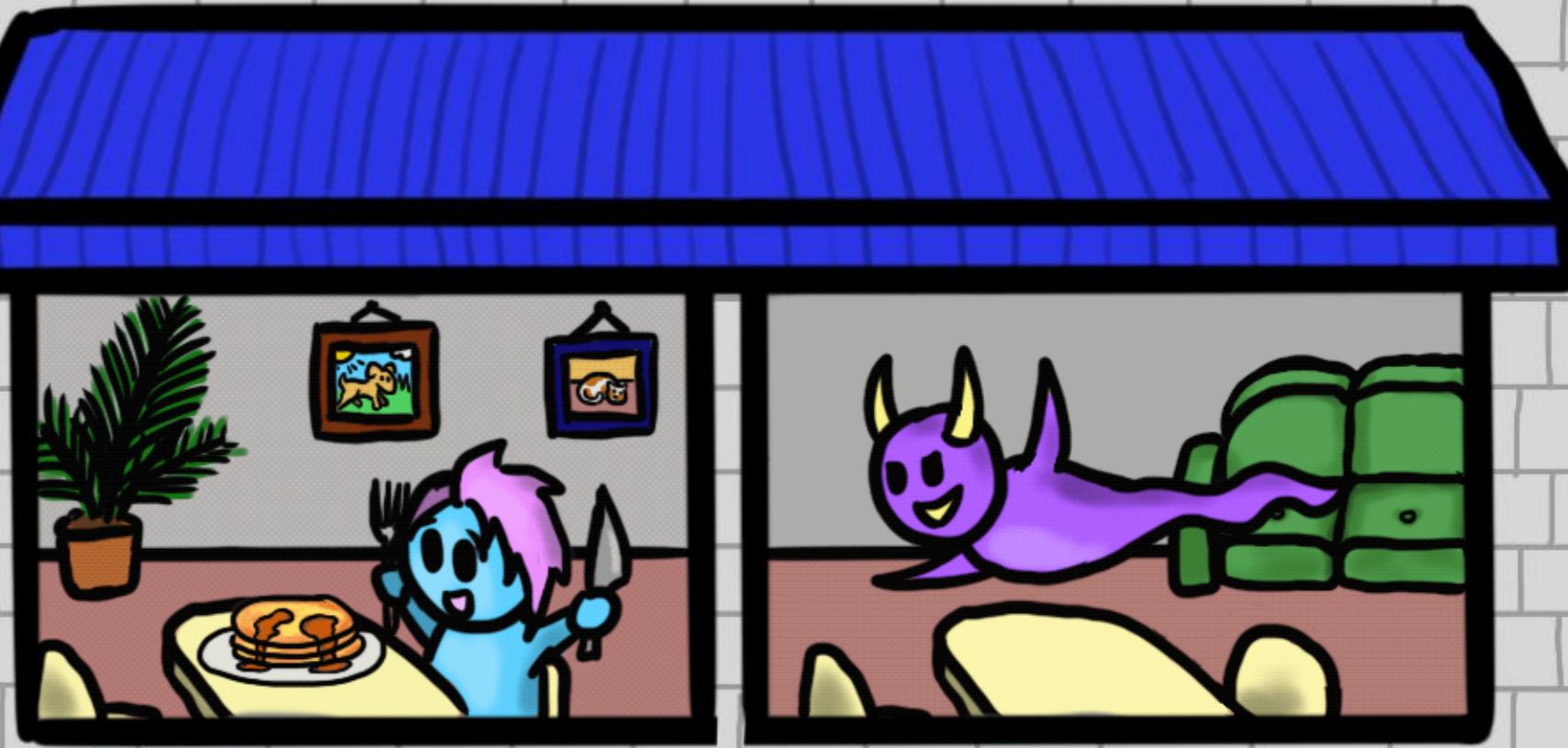


# I HOP

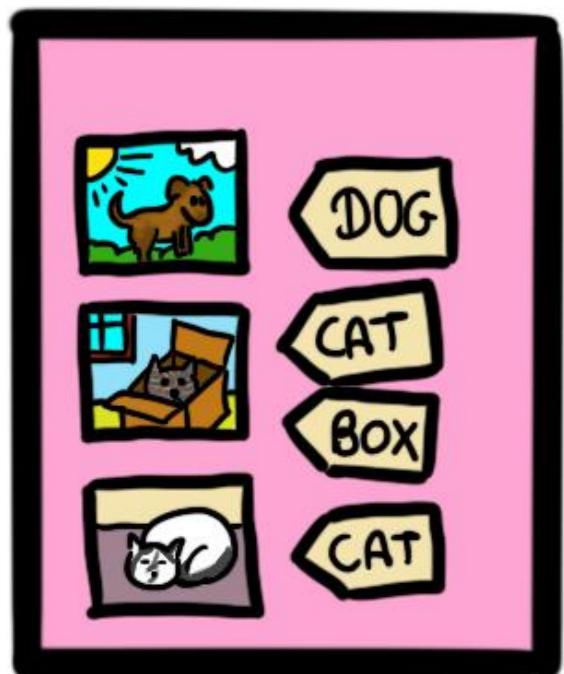
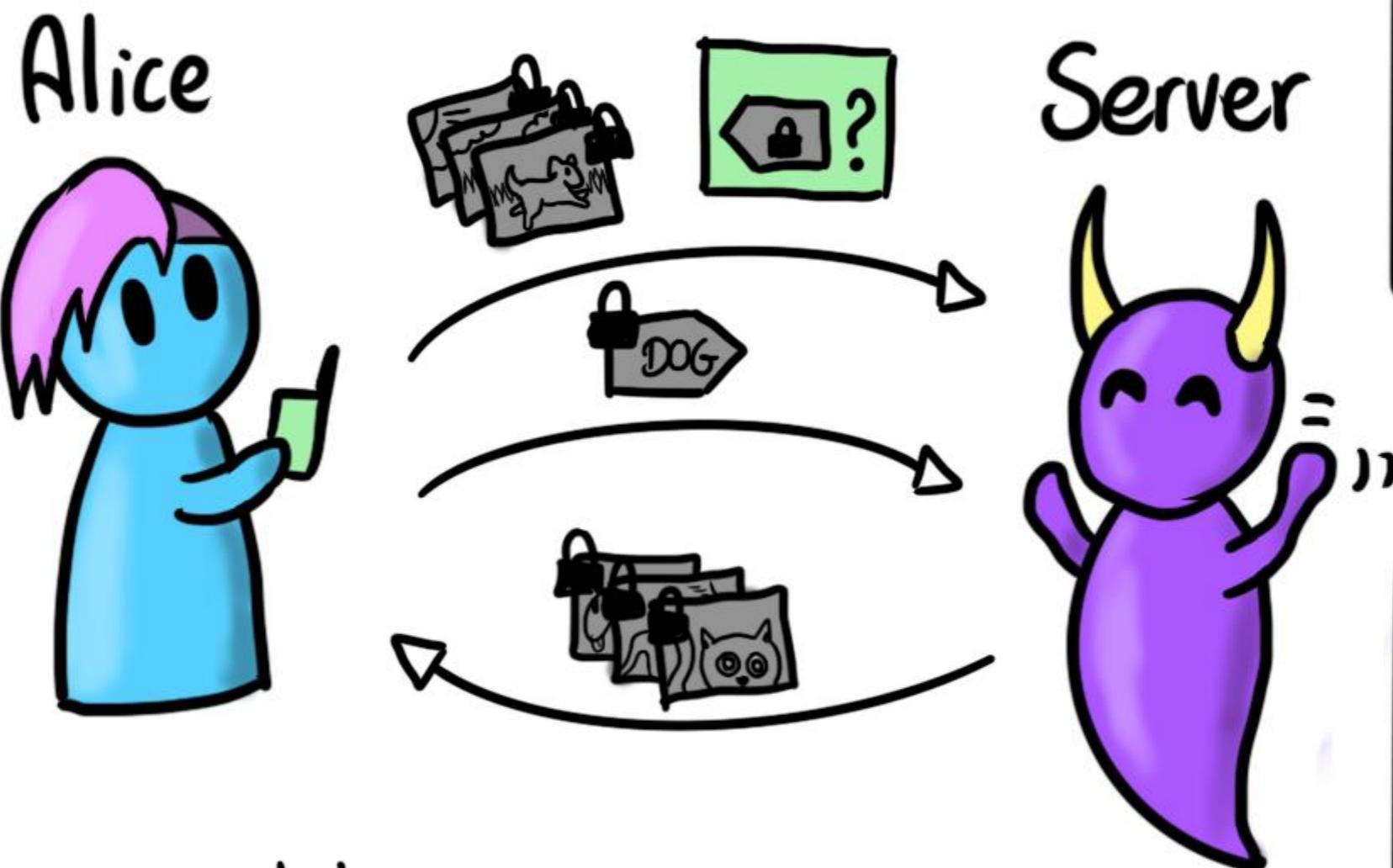
Improved Statistical  
Query Recovery against  
Searchable Encryption through  
Quadratic Optimization



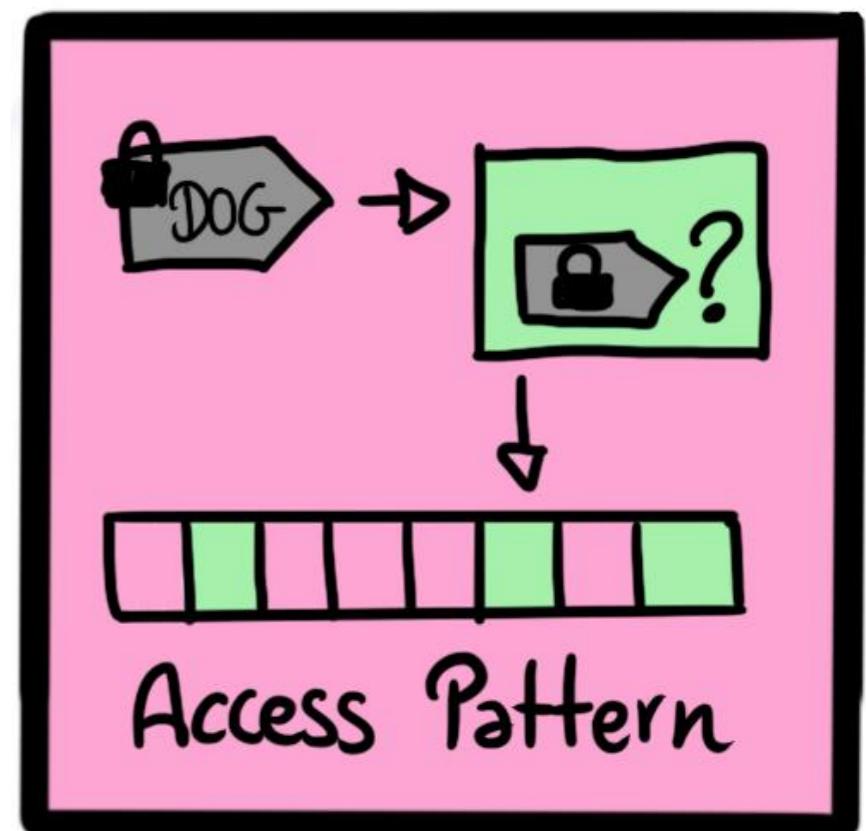
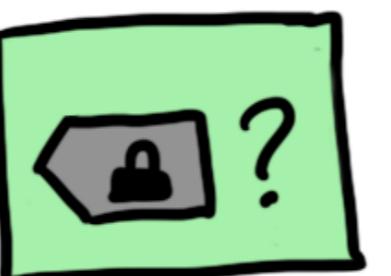
University of Waterloo

CrySP

# Overview: Searchable Encryption



Encrypted  
Search index

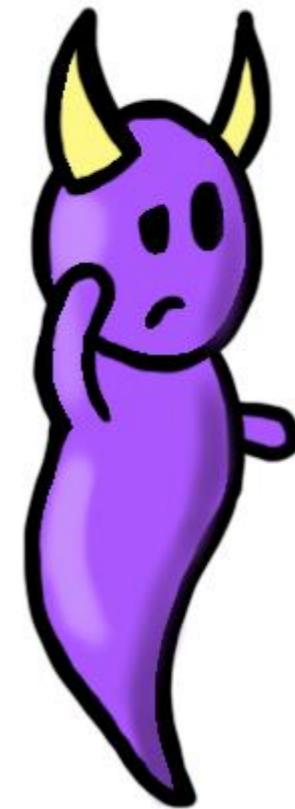
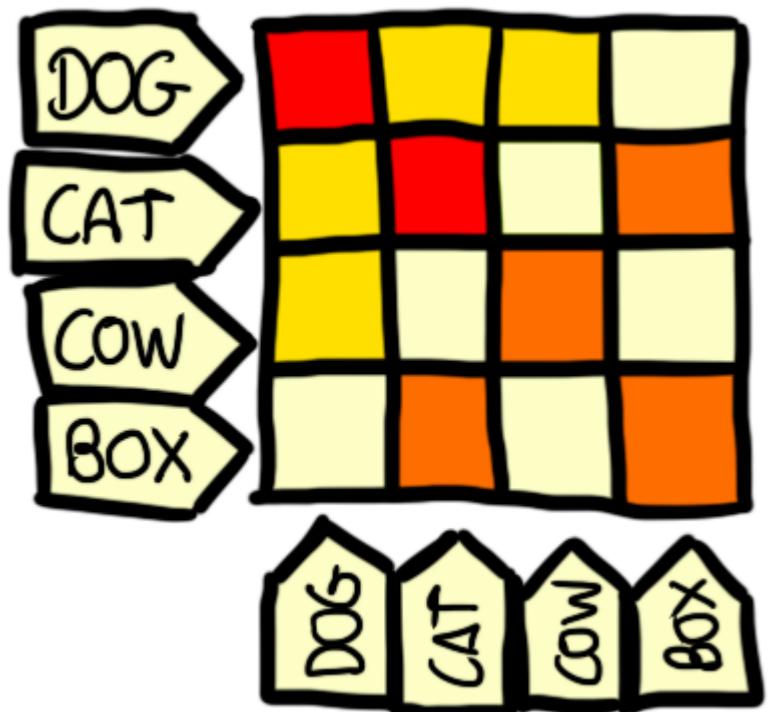


# Leakage & Adversary Model

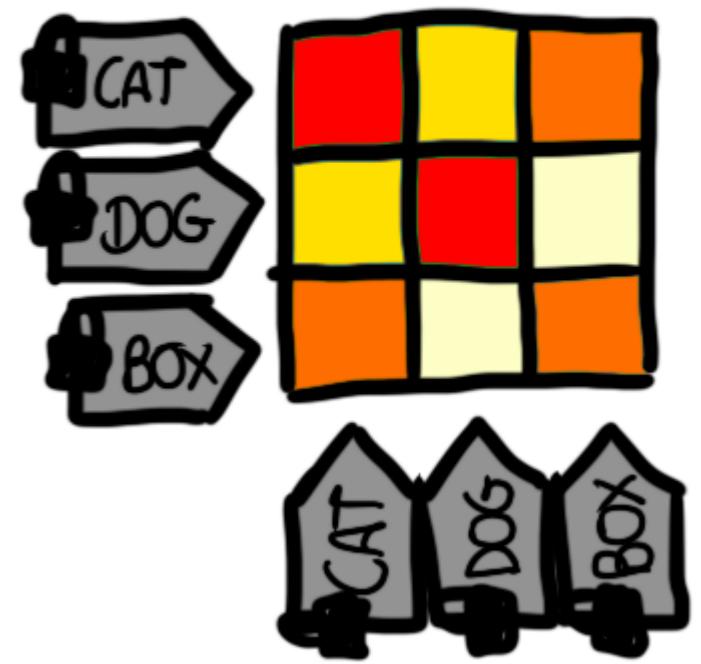
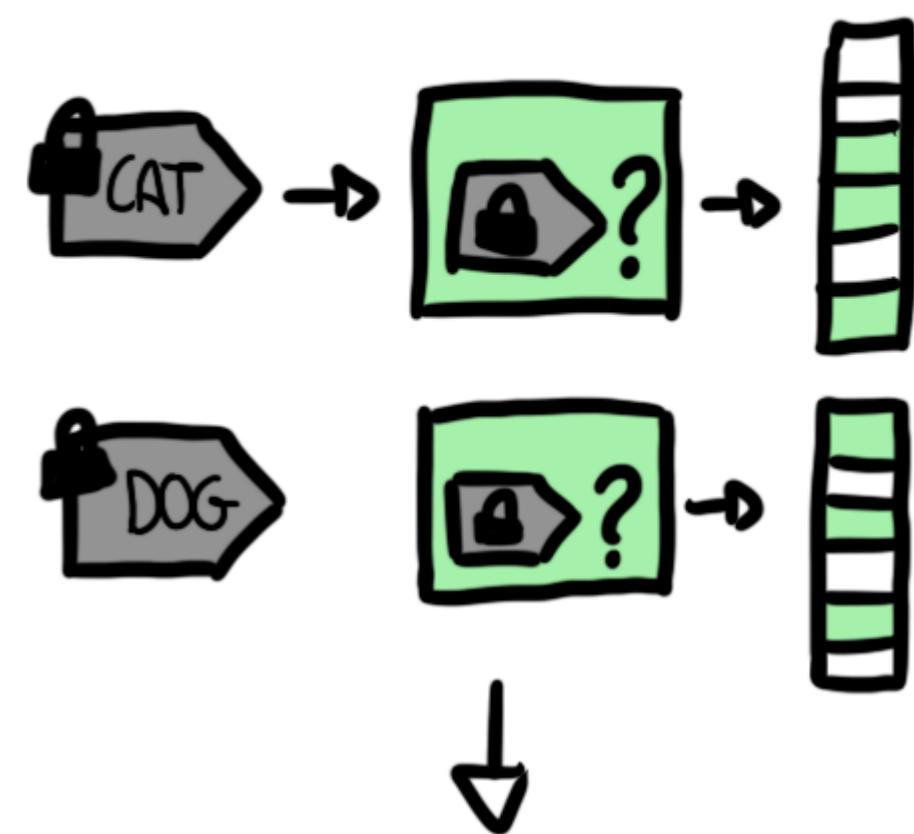
## Auxiliary Information



↓ Volume  
co-occurrence



## Observations

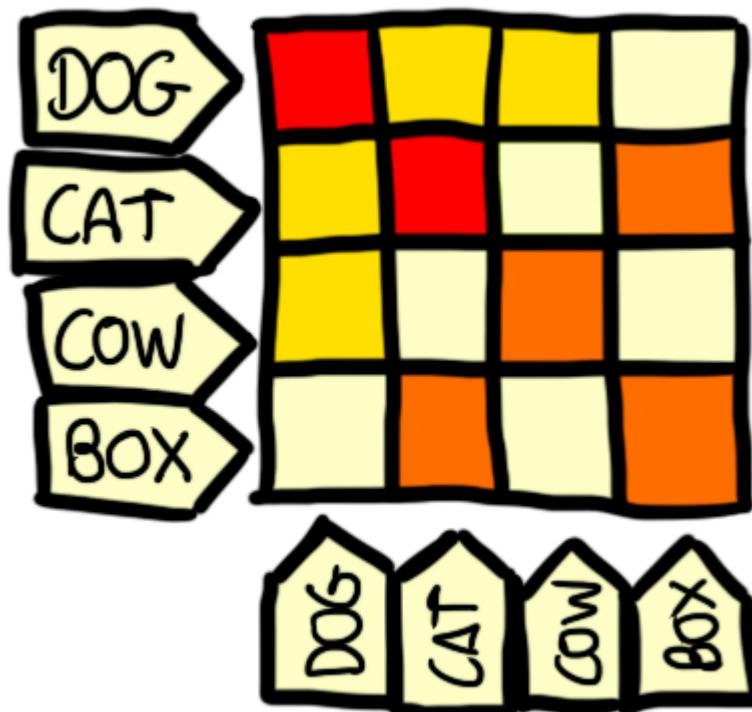


# Leakage & Adversarial

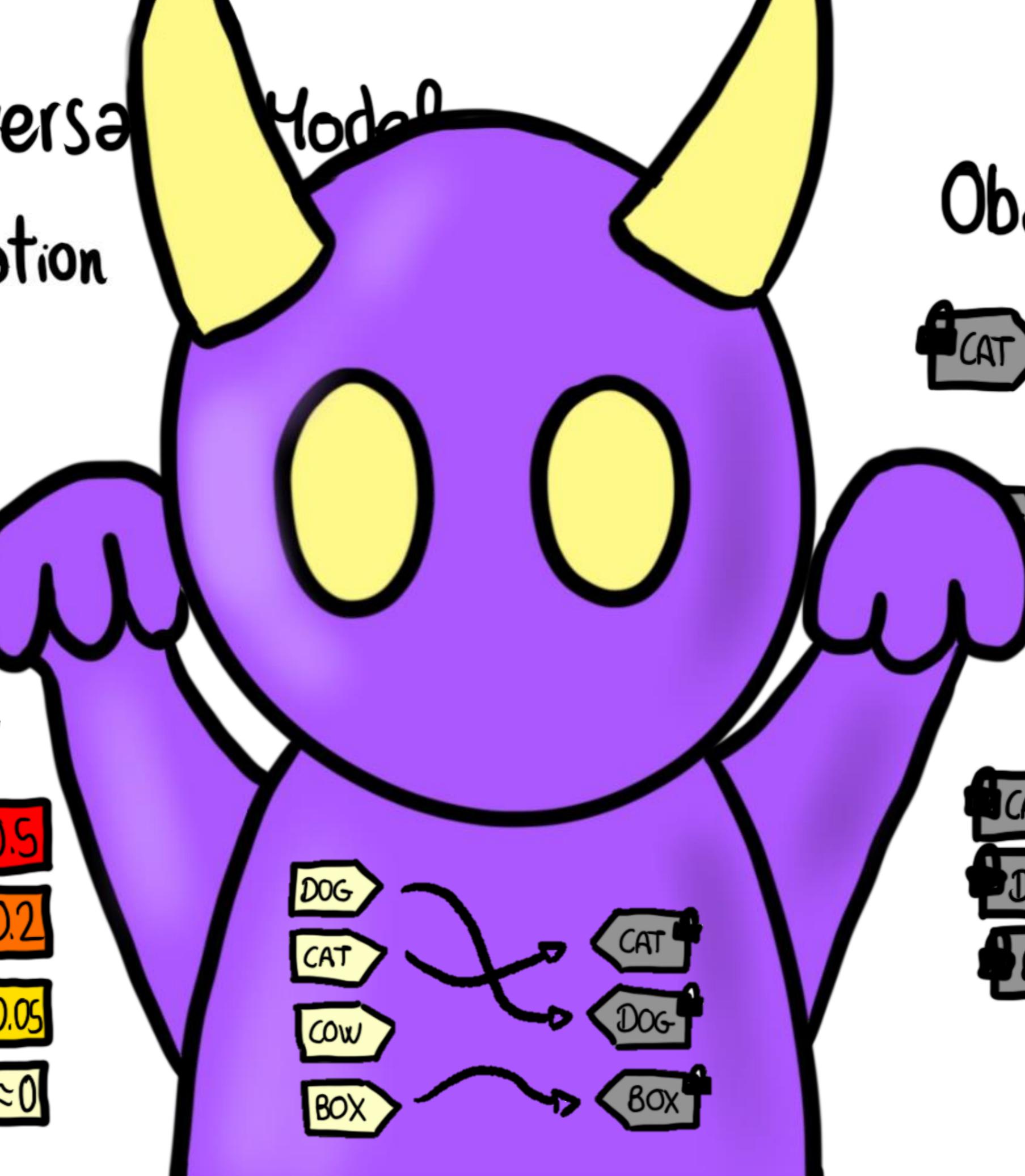
## Auxiliary Information



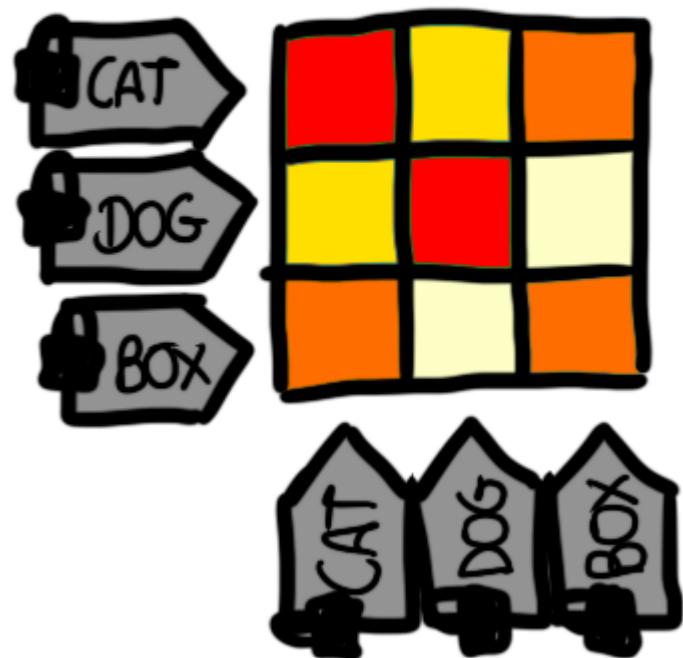
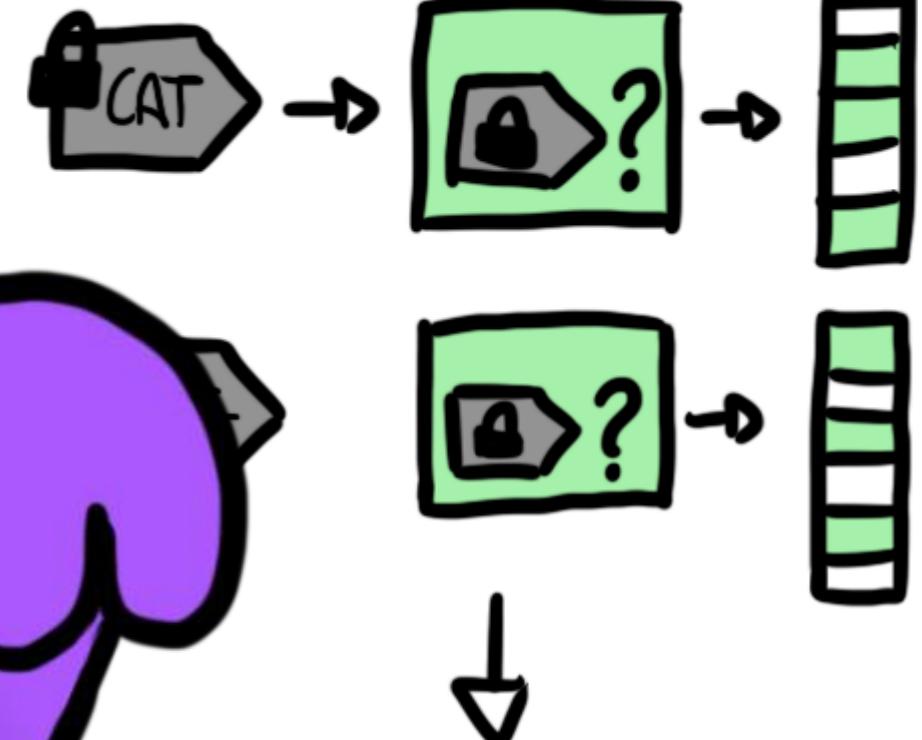
↓ Volume  
co-occurrence



↑↑ 0.5  
↑ 0.2  
↓ 0.05  
↓↓ ≈ 0

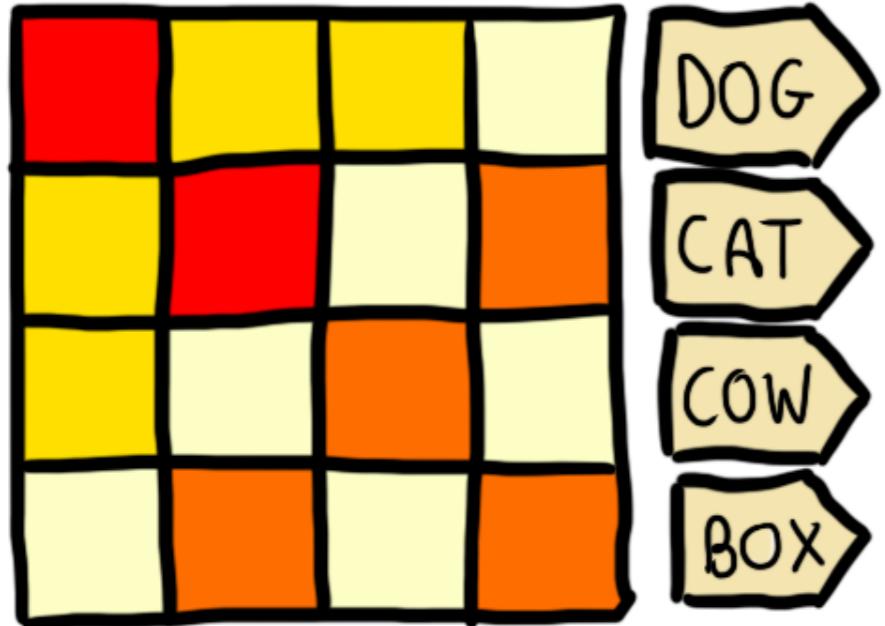


## Observations

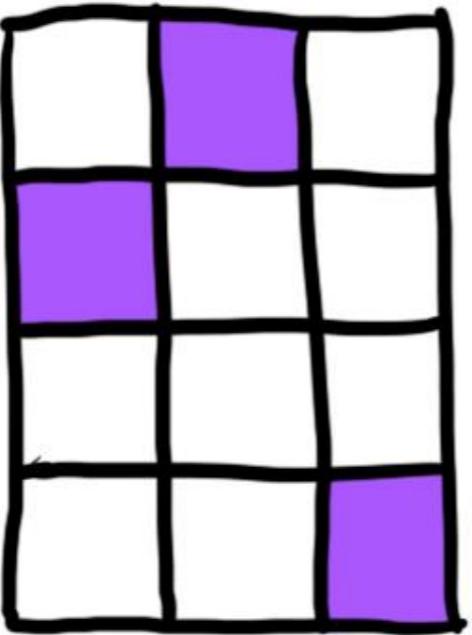


# Quadratic Assignment Problem (QAP)

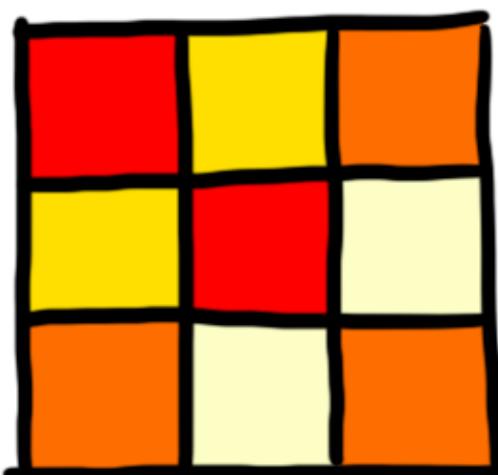
$\tilde{V}(n \times n)$  (AUX)



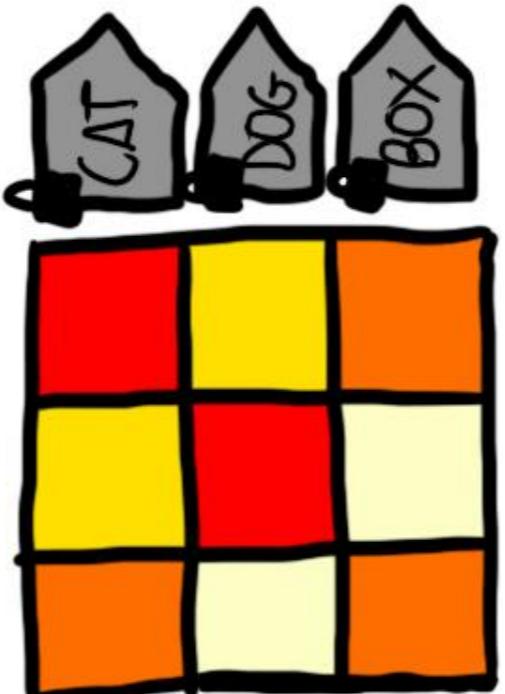
$P(n \times m)$



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



(OBS)



$V(m \times m)$

$$P = \underset{P \in \mathcal{P}}{\operatorname{argmin}} \sum_{i,i'} \sum_{j,j'} C_{i,i',j,j'} \cdot P_{ij} \cdot P_{i'j'}$$

Examples

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

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

↳ Convex-concave rel.

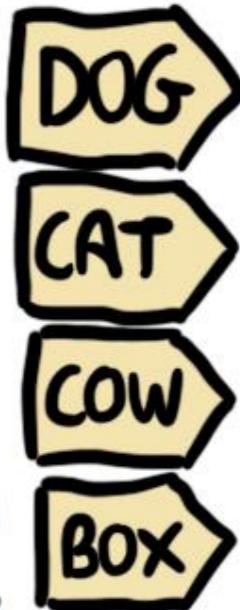
- [1] Islam et al. Access pattern disclosure on searchable encryption: Ramification, attack and mitigation. NDSS 2012.
- [2] Pouliot and Wright. The shadow nemesis: Inference attacks on efficiently deployable, efficiently searchable encryption. CCS 2016



# Linear Assignment Problem (LAP)

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

Red	Yellow	Yellow	Yellow
Yellow	Red	White	Orange
White	Orange	Orange	White
White	Orange	White	Orange



$P(n \times m)$

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

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



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	Orange
Yellow	Red	White	White
White	White	White	White

$V(m \times m)$

SAP [3]

$$P = \underset{P \in \mathcal{P}}{\operatorname{arg\min}} \sum_{i} \sum_{j} d_{ij} \cdot P_{ij}$$

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



But lots of wasted information



Hungarian algorithm

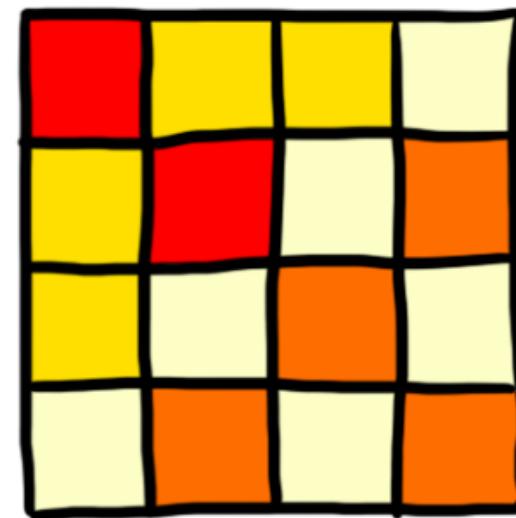
[3] Oya and Kerschbaum. *Hiding the access pattern is not enough: Exploiting search pattern leakage in searchable encryption*. USENIX 2021

Efficient!



# IHOP: Iteration Heuristic for (Quadratic) Optimization Problems

$\tilde{V}$  (aux)

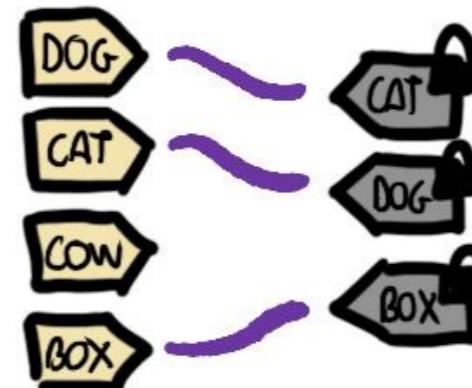


P



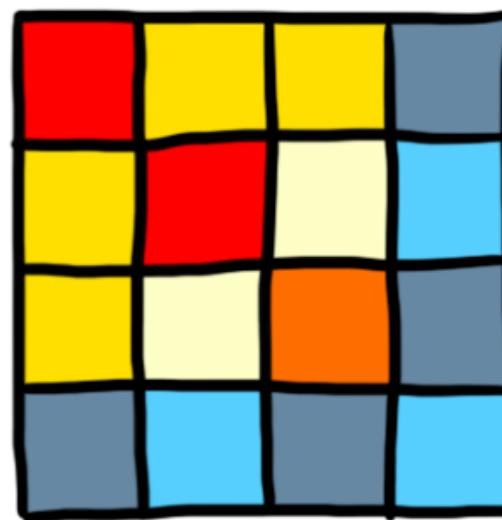
V (obs)

① Full assignment



# IHOP: Iteration Heuristic for (Quadratic) Optimization Problems

$\tilde{V}$  (aux)

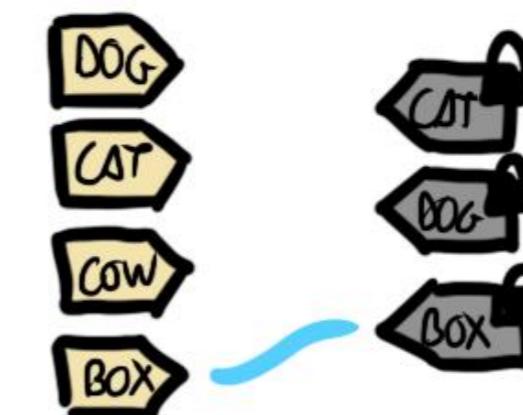
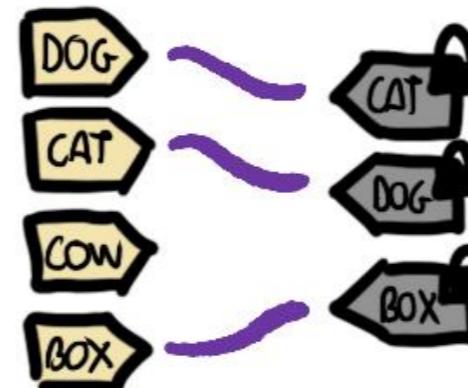


P

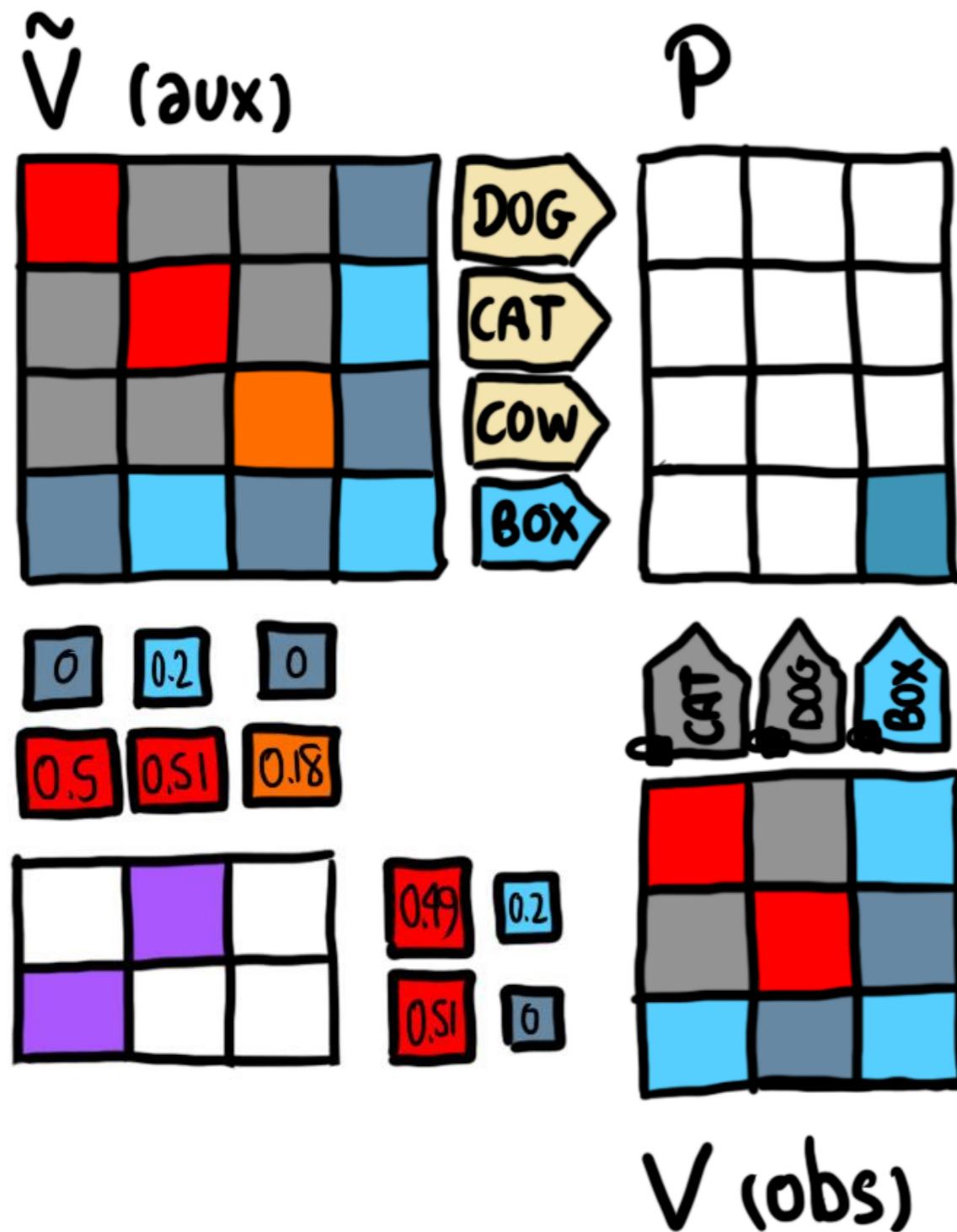


V (obs)

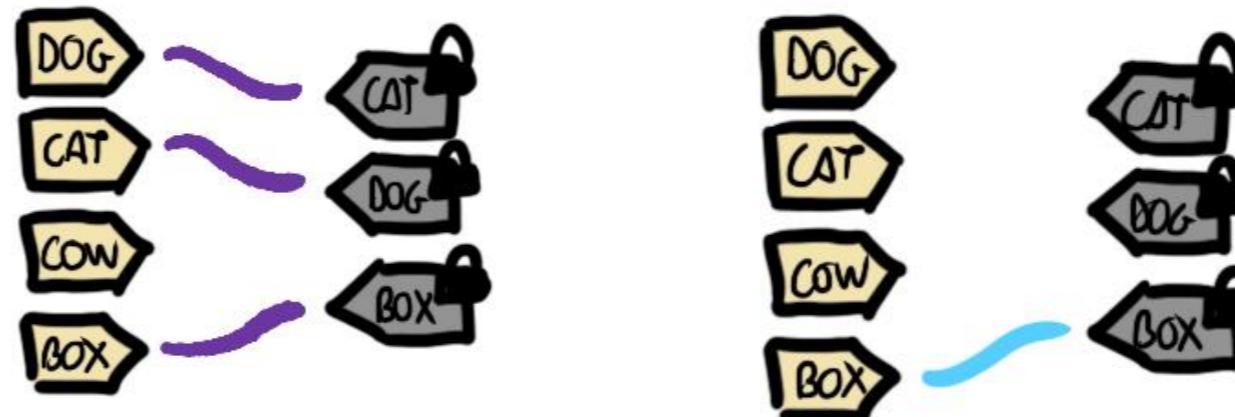
- ① Full assignment
- ② Freeze some "~~"



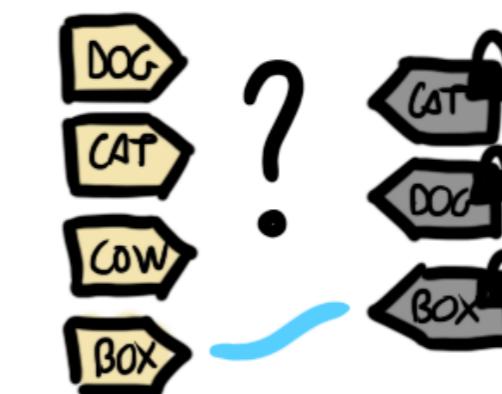
# IHOP: Iteration Heuristic for (Quadratic) Optimization Problems



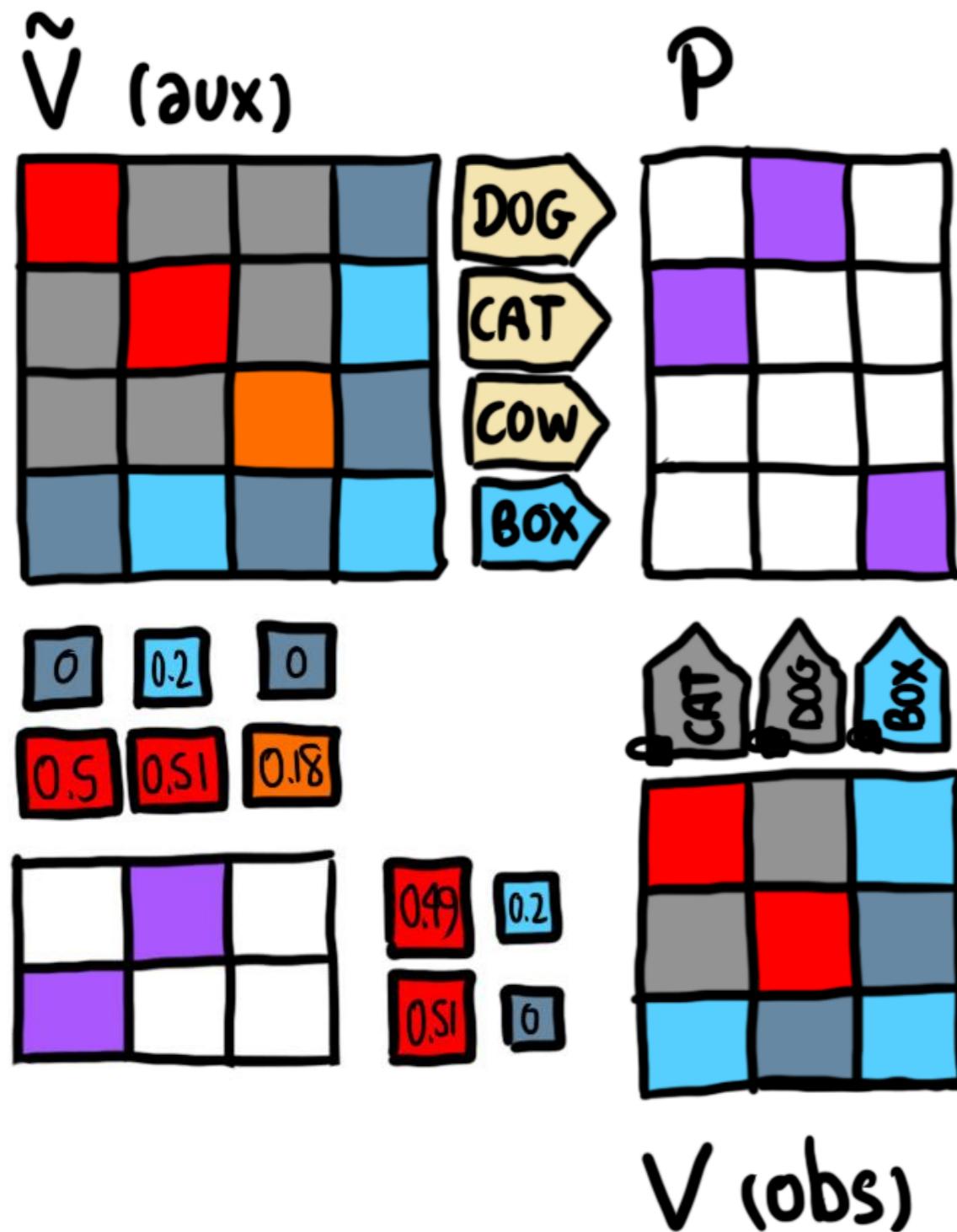
① Full assignment    ② Freeze some "~~"



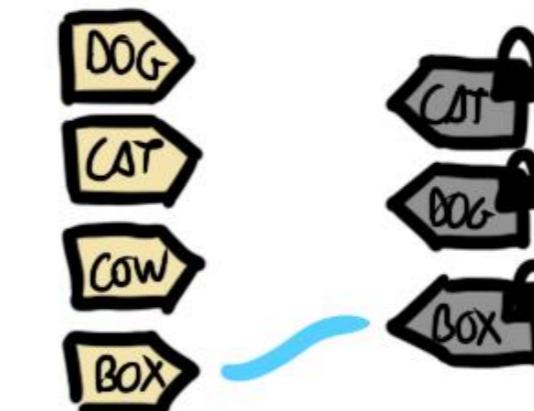
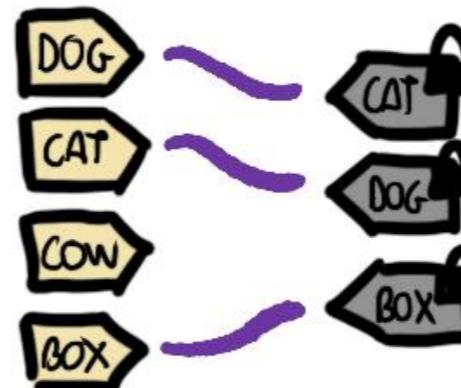
③ LAP w/ frozen



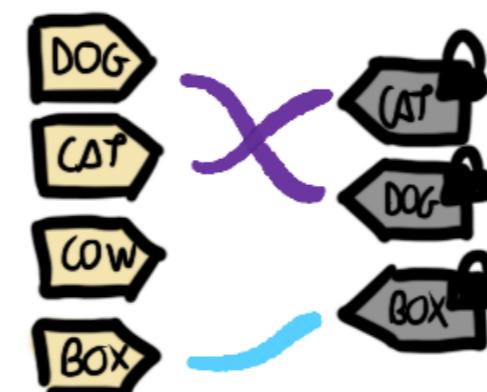
# IHOP: Iteration Heuristic for (Quadratic) Optimization Problems



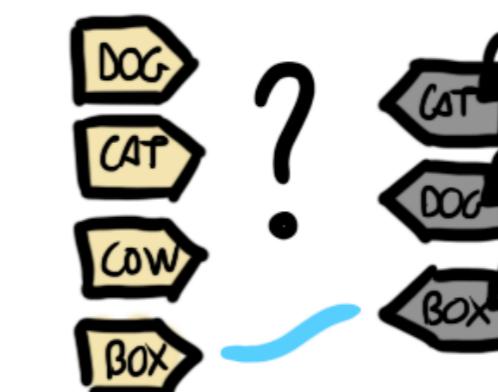
① Full assignment    ② Freeze some "~~"



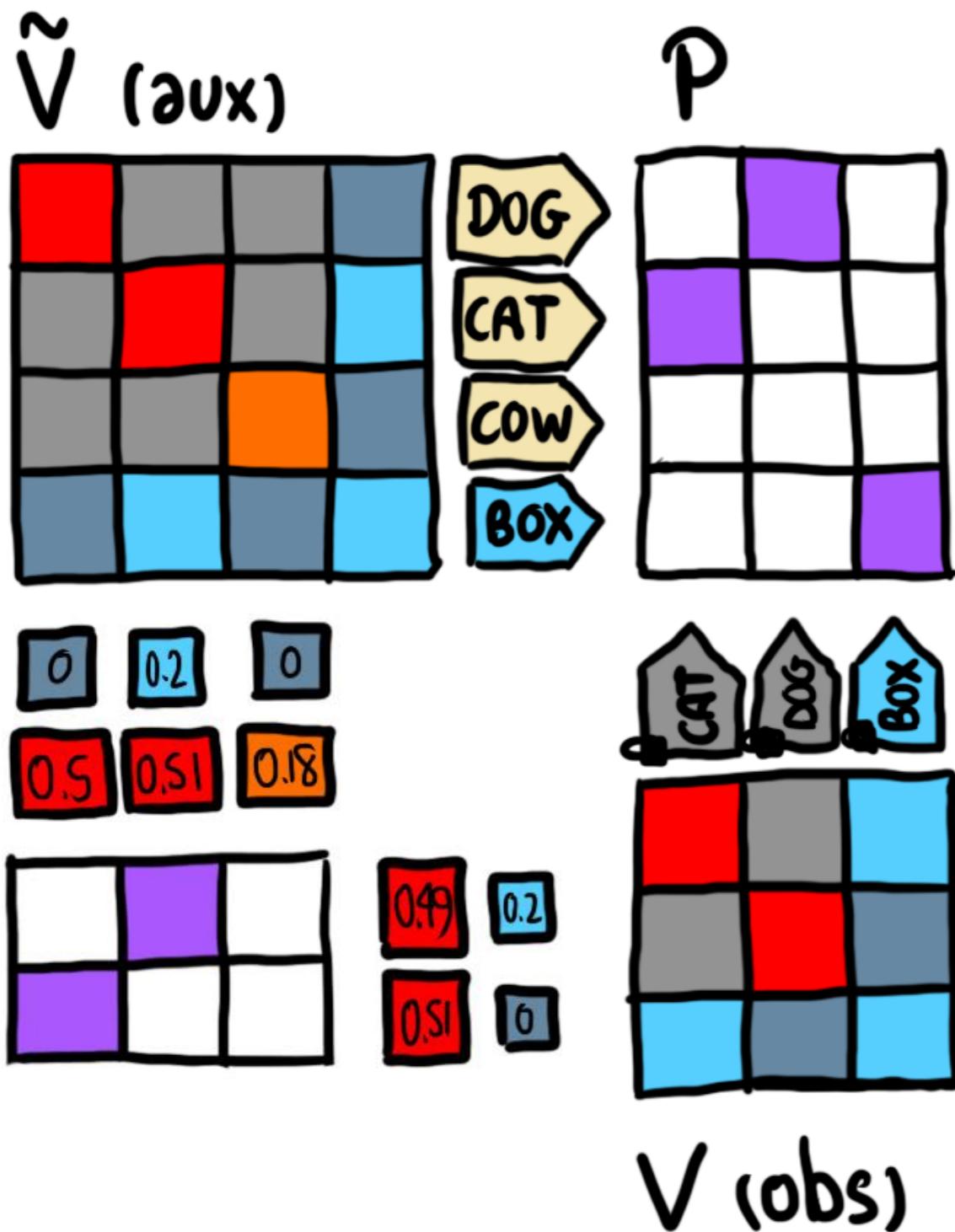
④ Solve LAP



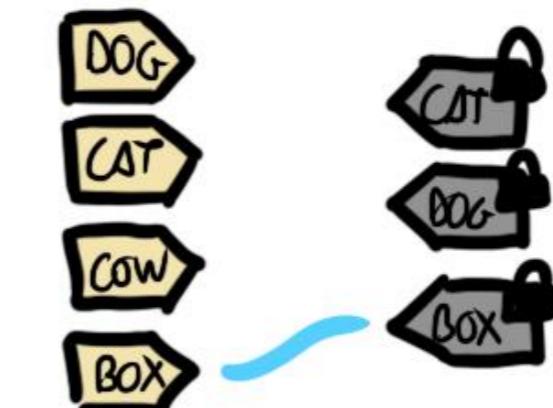
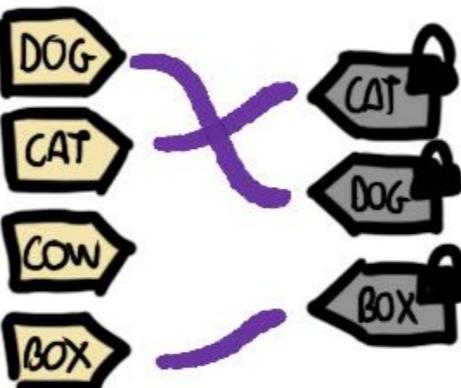
③ LAP w/ frozen



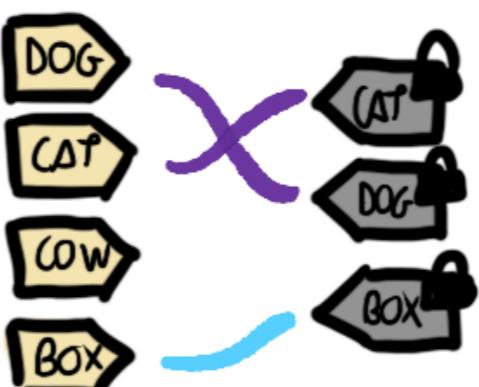
# IHOP: Iteration Heuristic for (Quadratic) Optimization Problems



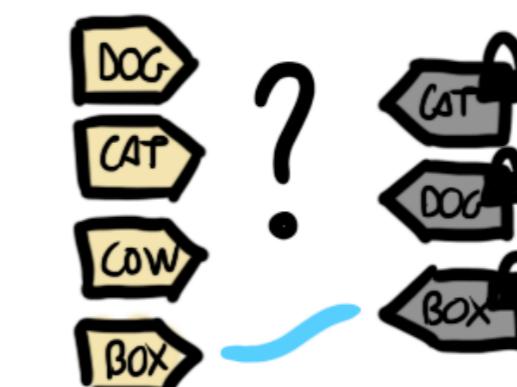
- ① Full assignment
- ② Freeze some "~~"



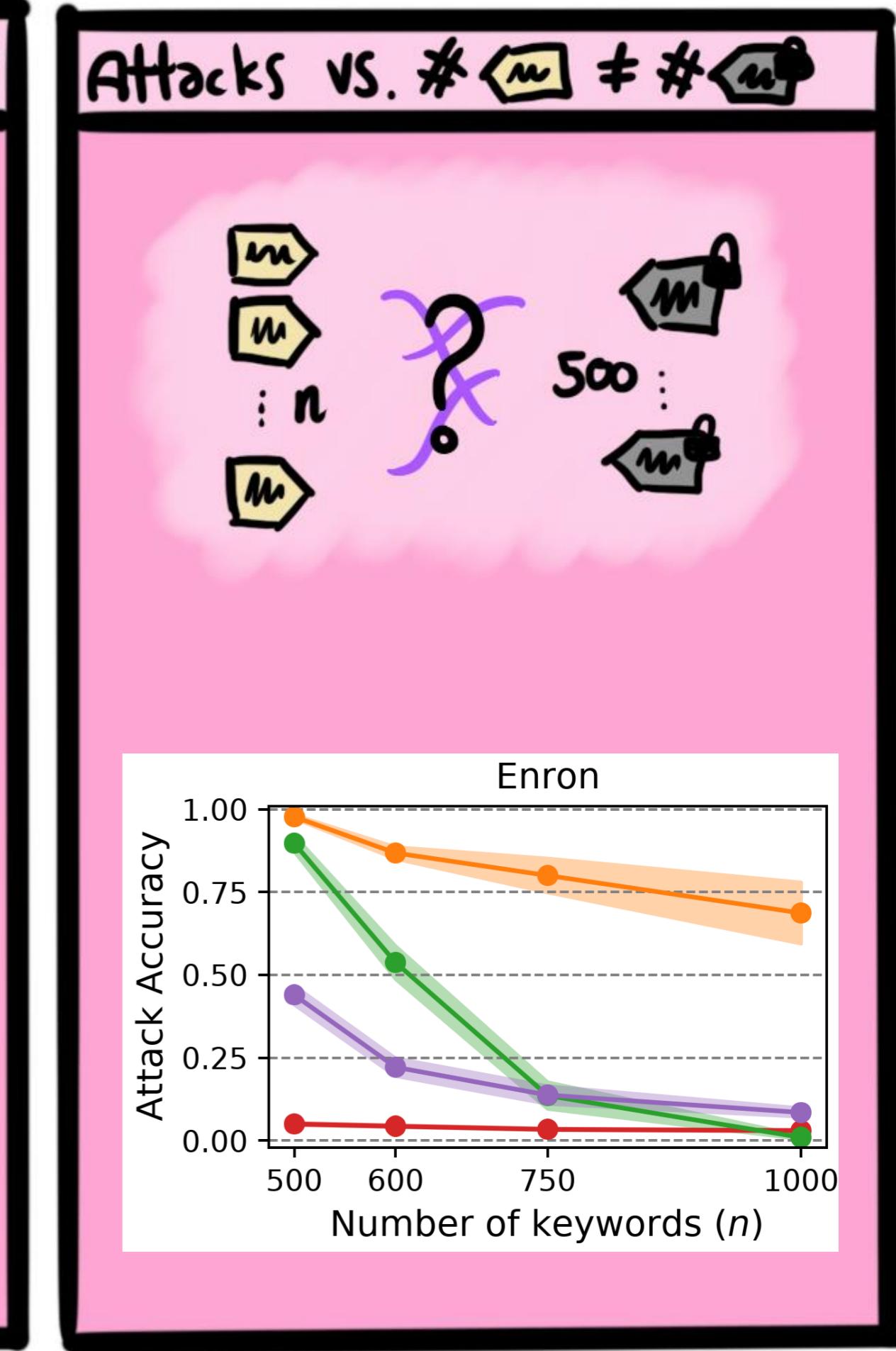
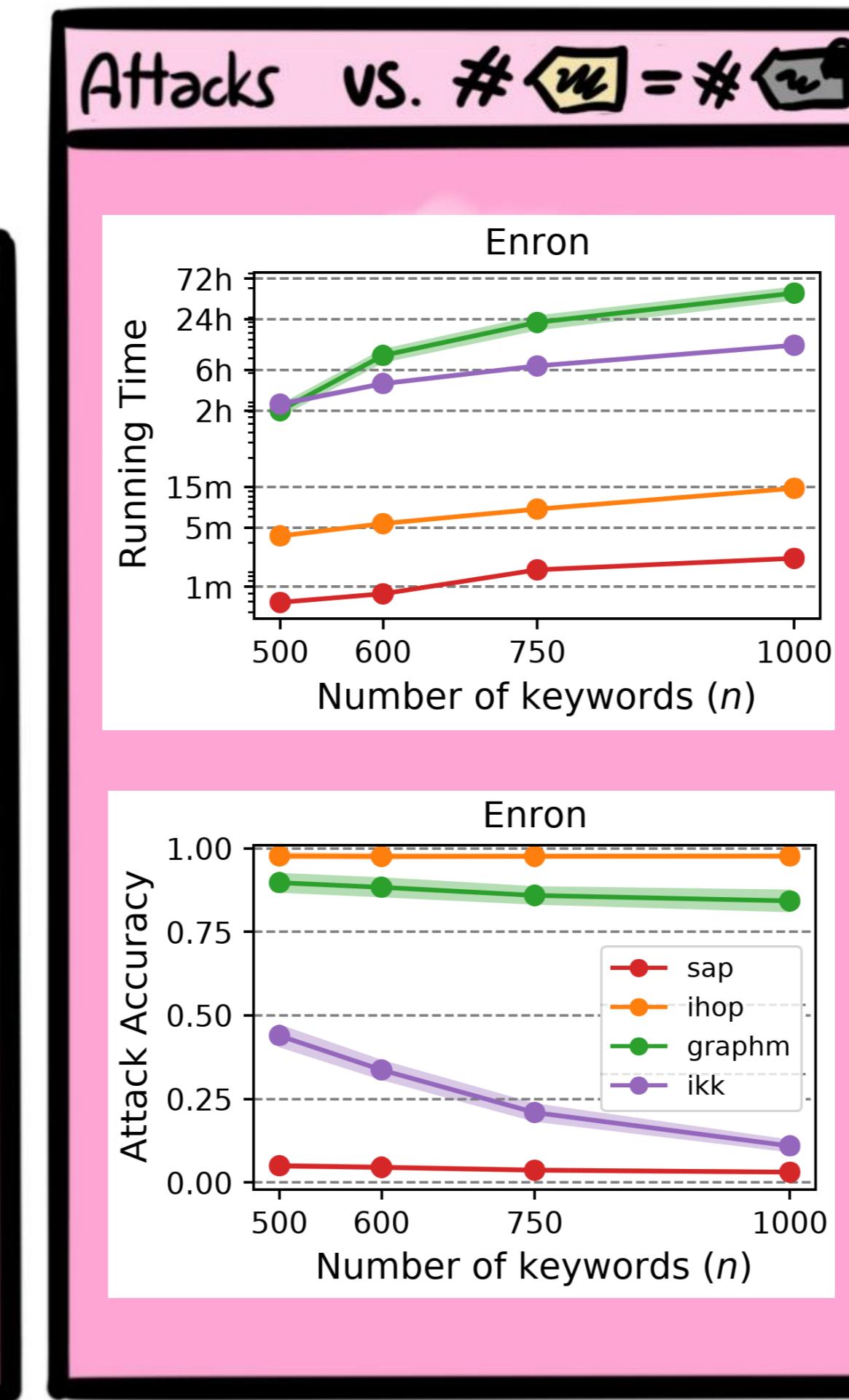
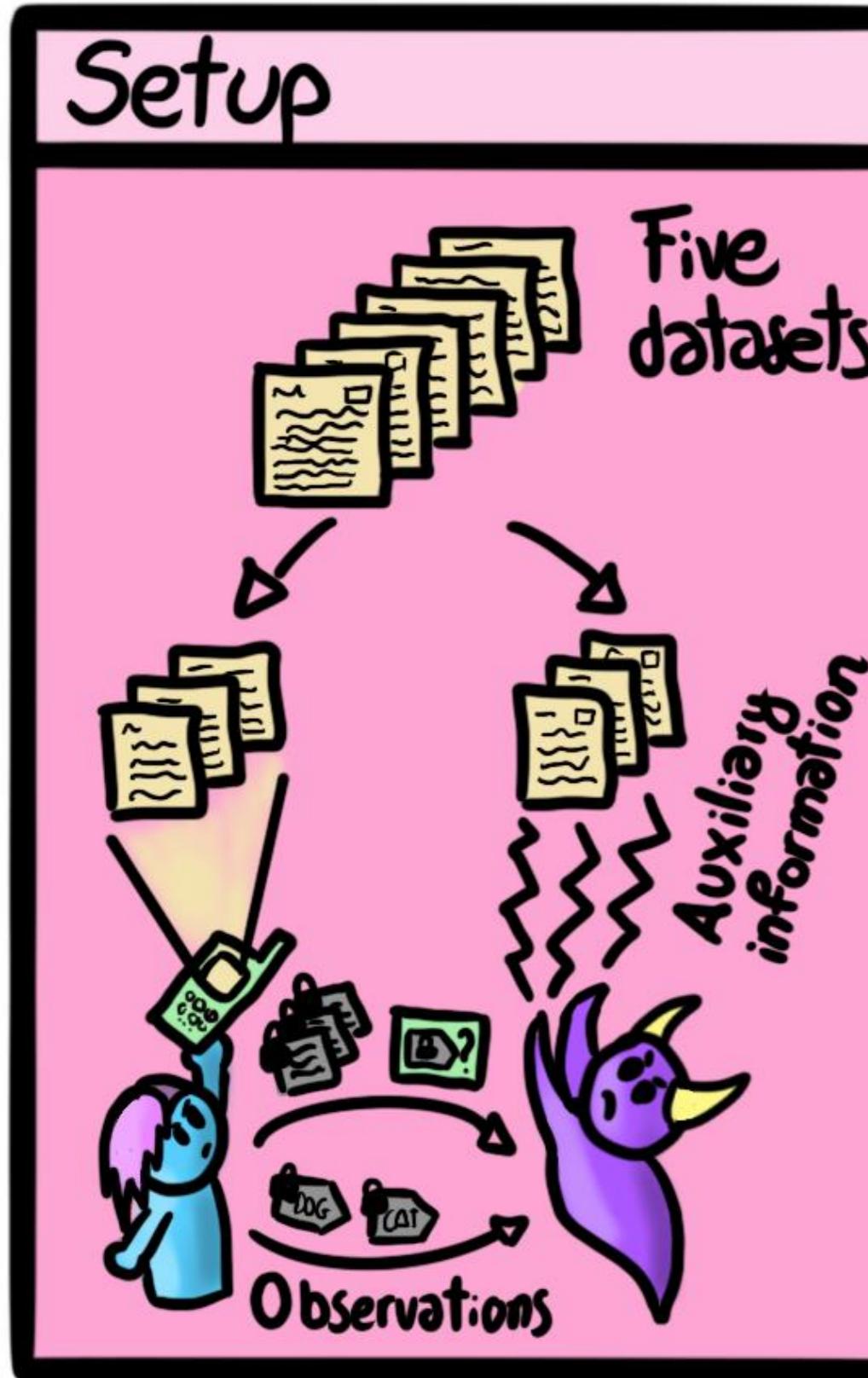
- ④ Solve LAP



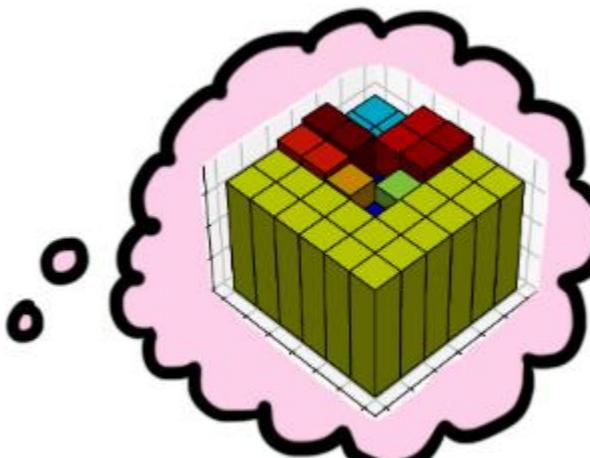
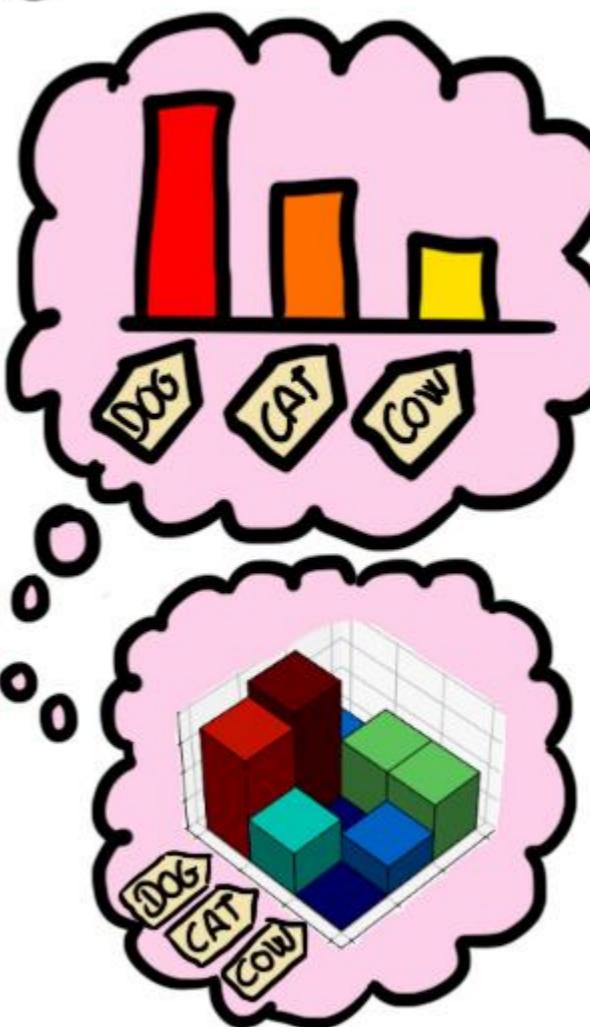
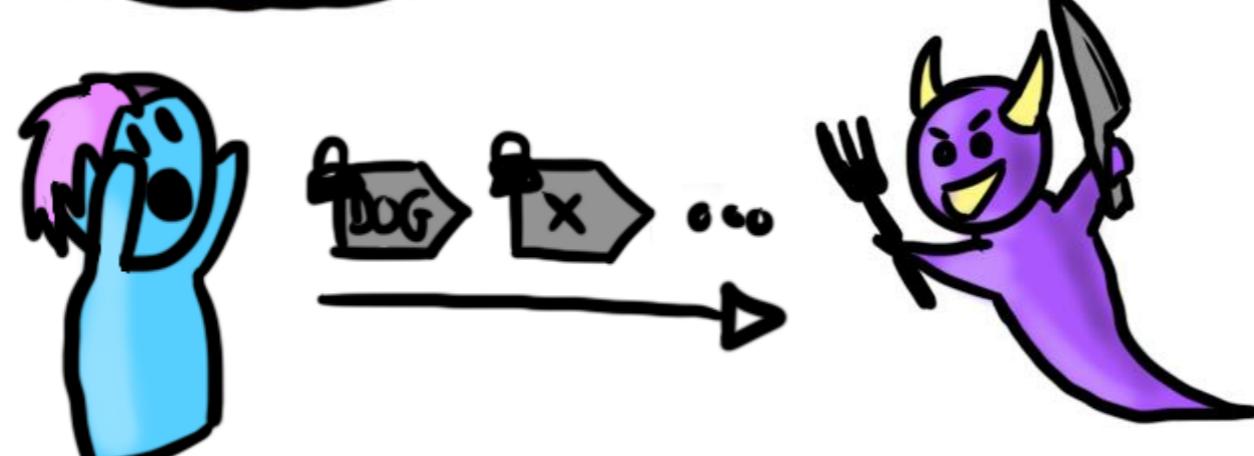
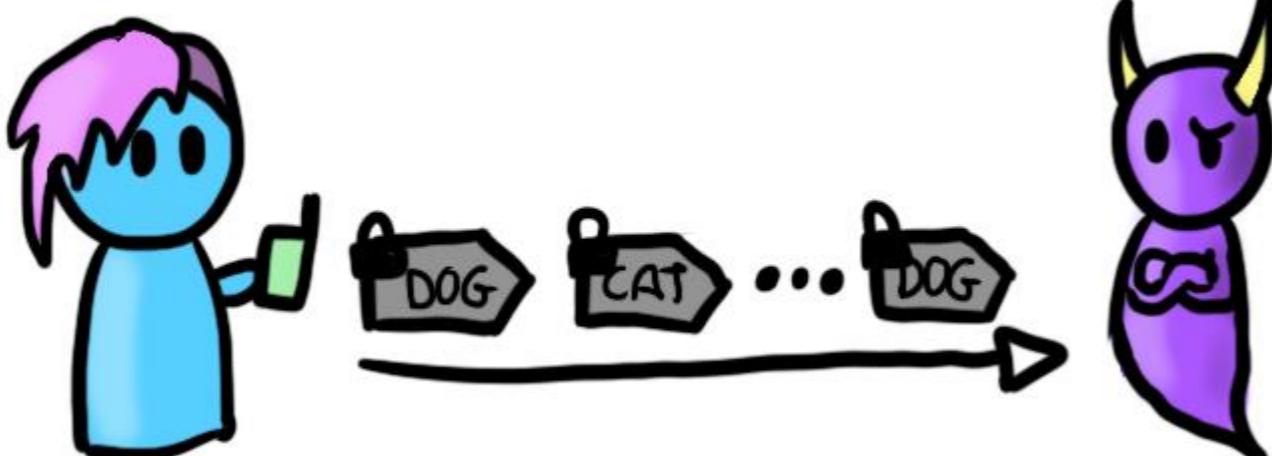
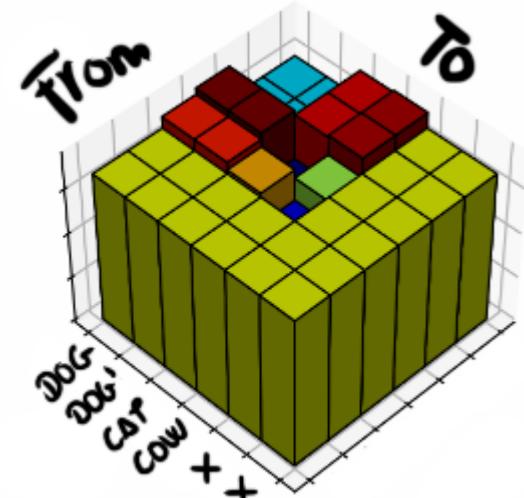
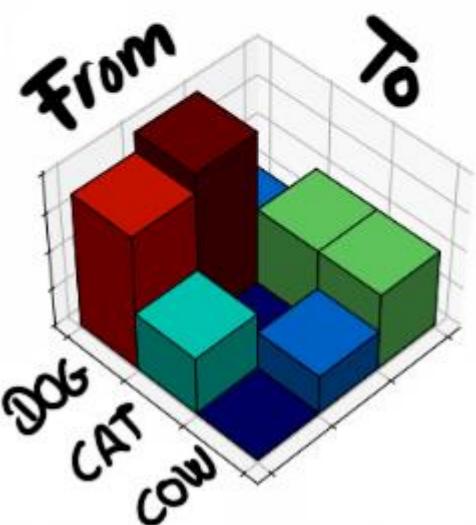
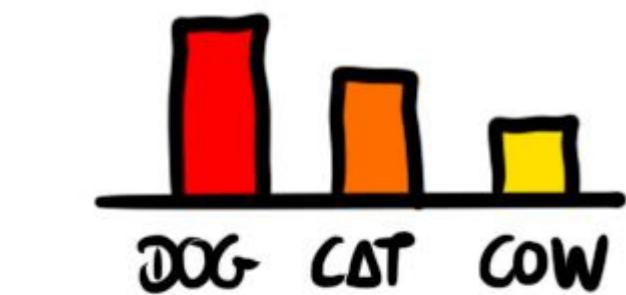
- ③ LAP w/ frozen



# Some experiments



# IHOP vs. Pancake (Very briefly)



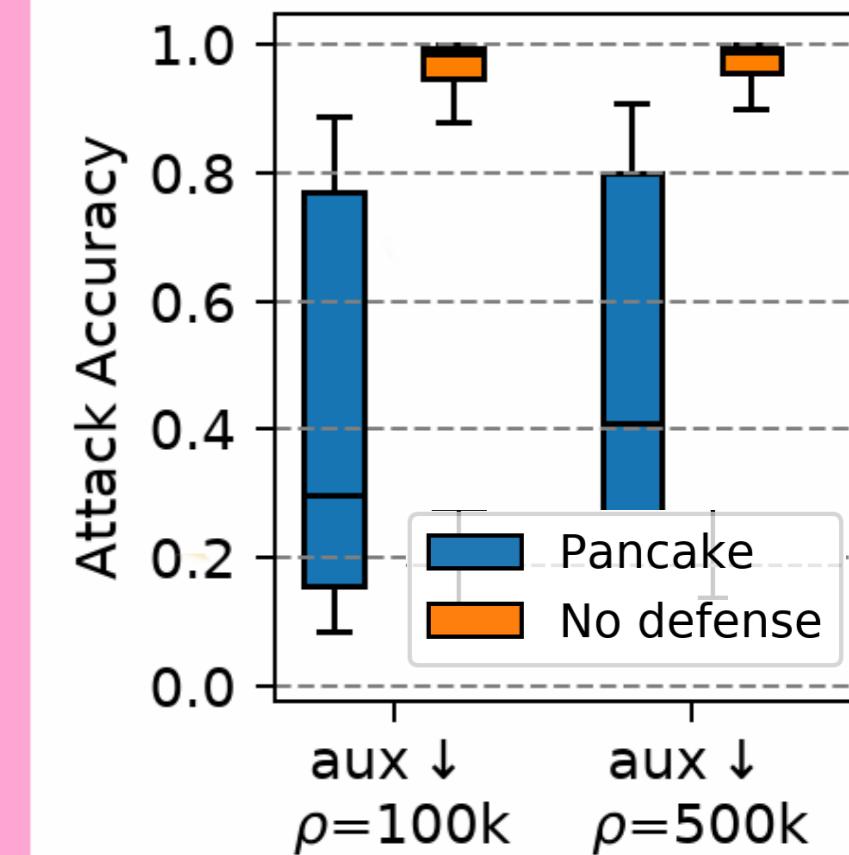
## Some Results

Wikipedia Datasets

500 documents



1000 replicas



# I HOP

New! **FASTER!**

Statistical Recovery Query  
Attack

**FLEXIBLE**

**MORE ACCURATE**

Questions?

Simon.oya@uwaterloo.ca

