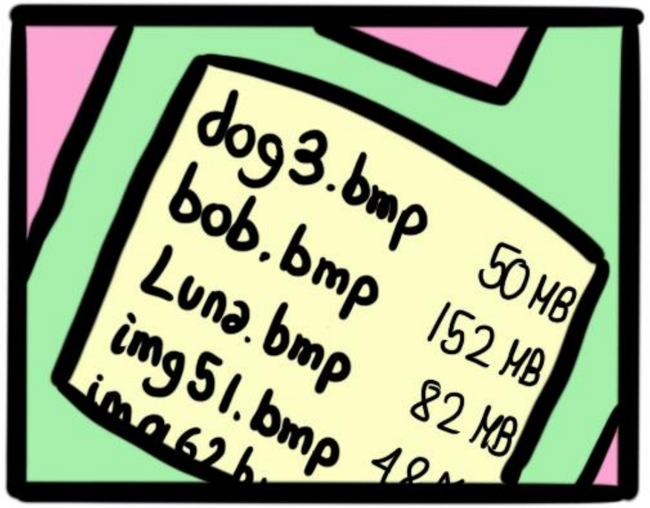
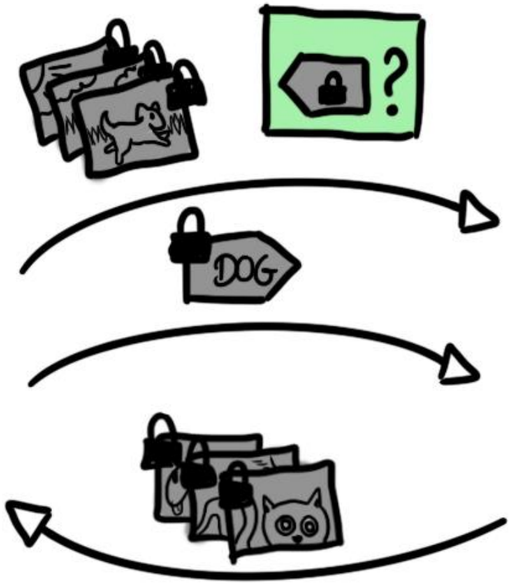

IHOP
Simon Oya
Florian Kerschbaum
Improved Statistical Query Recovery against Searchable Encryption through Quadratic Optimization
University of Waterloo
CrySP

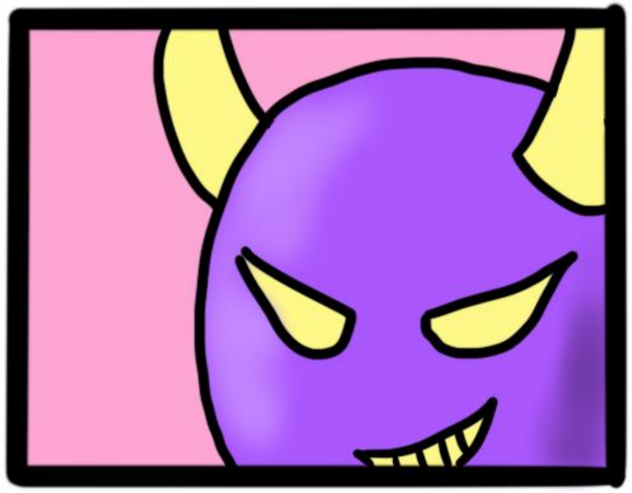
Overview: Searchable Encryption

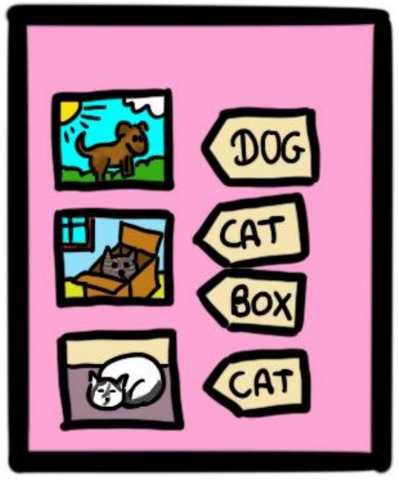


Alice

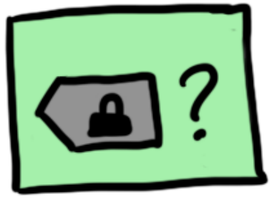


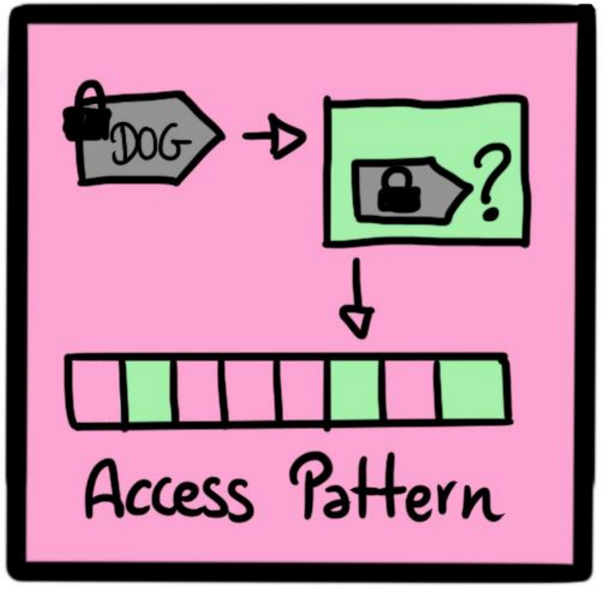
Server





Encrypted search index

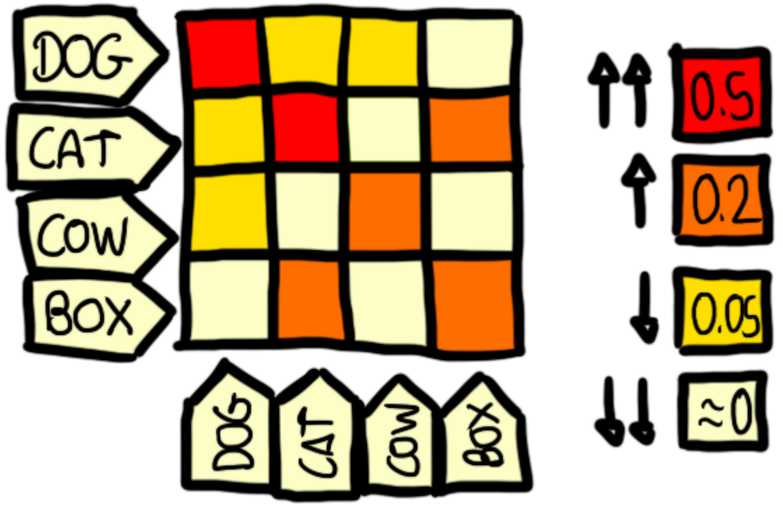




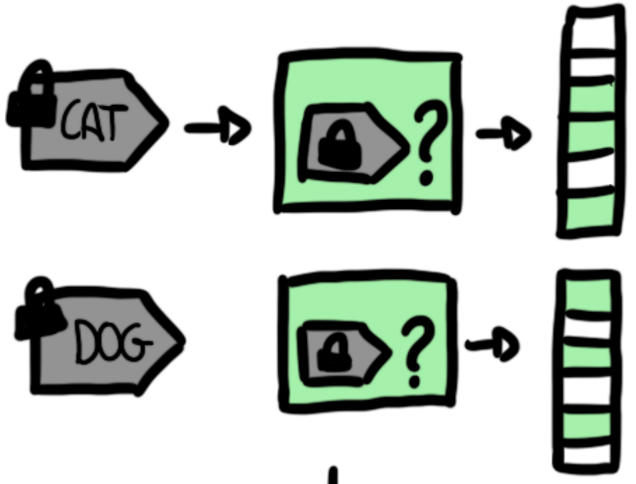
Leakage & Adversary Model

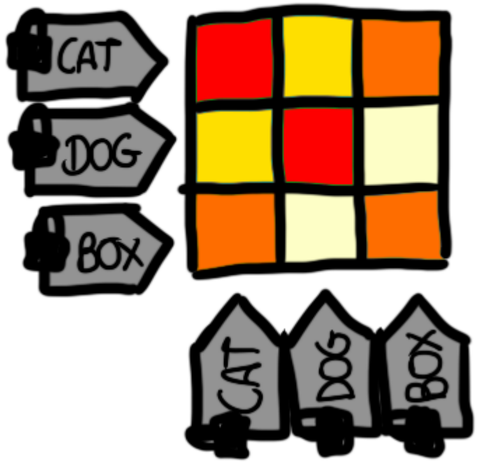
Auxiliary Information

↓ Volume
co-occurrence



Observations

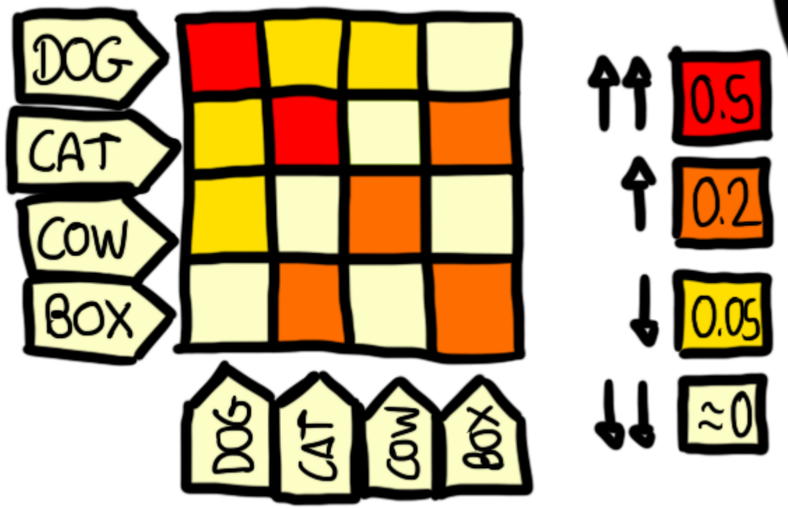


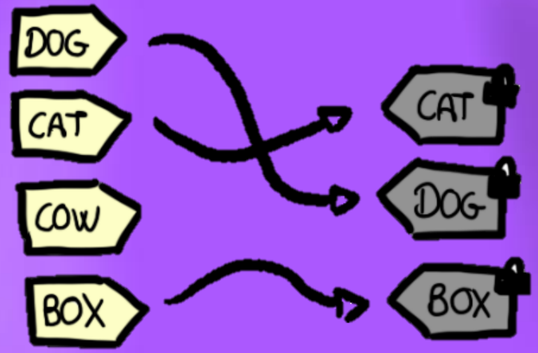


Leakage & Adversa Model

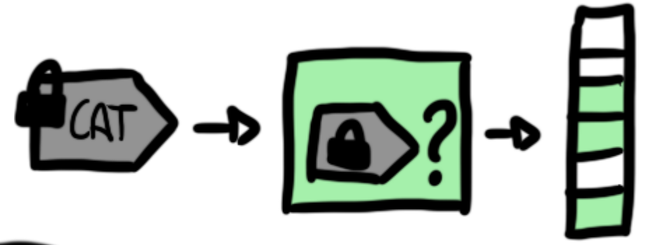
Auxiliary Information

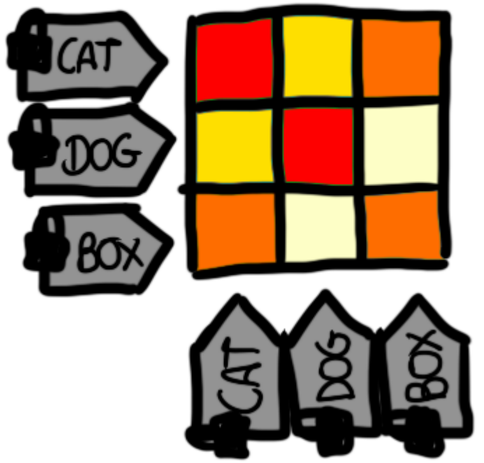
↓ Volume
co-occurrence



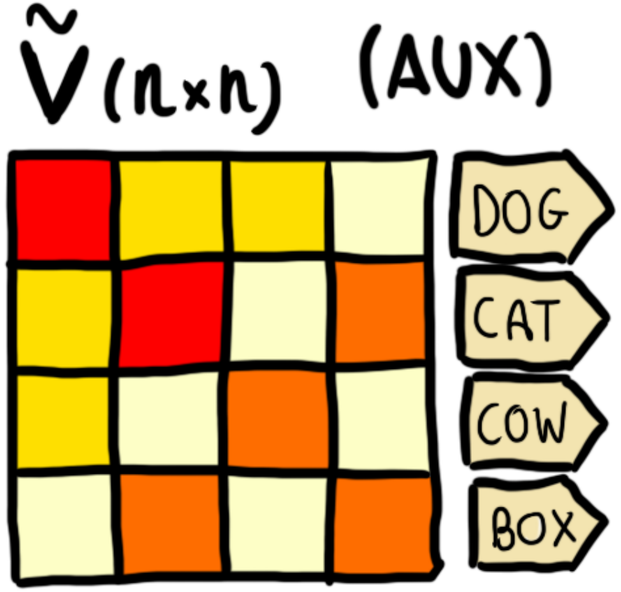


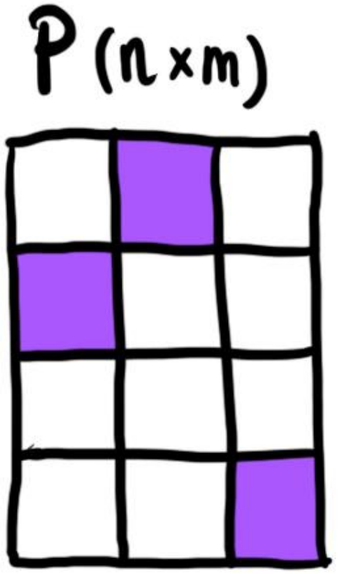
Observations





Quadratic Assignment Problem (QAP)





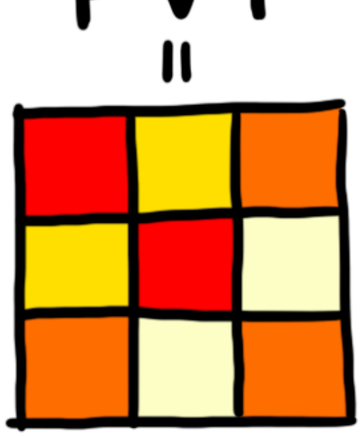
$$P = \underset{P \in \mathcal{P}}{\operatorname{argmin}} \sum_{i} \sum_{i'} C_{ii'jj'} \cdot P_{ij} \cdot P_{i'j'}$$

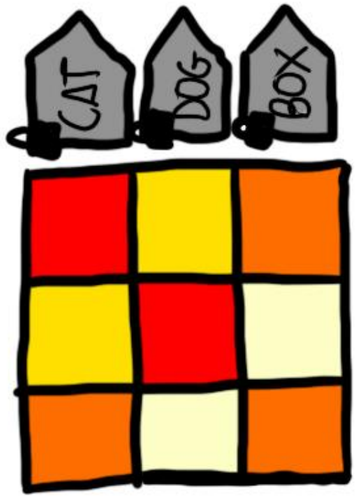
Examples

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

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

↳ Convex-concave rel.





(OBS)

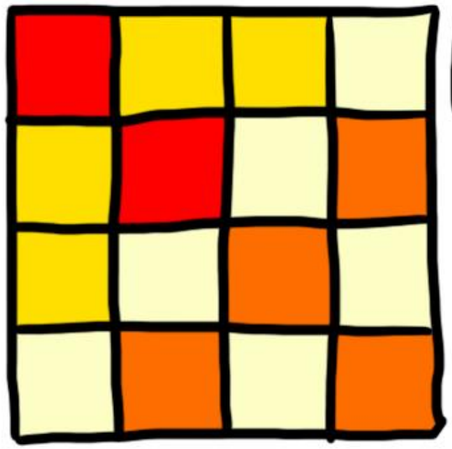
V (m×m)

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

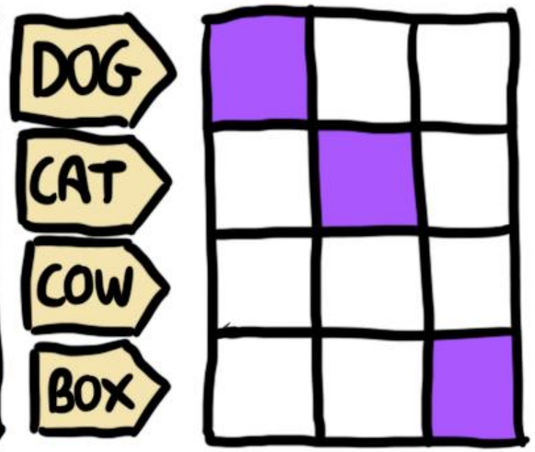
[2] Pouliot and Wright. *The shadow nemesis: Inference attacks on efficiently deployable, efficiently searchable encryption.* CCS 2016

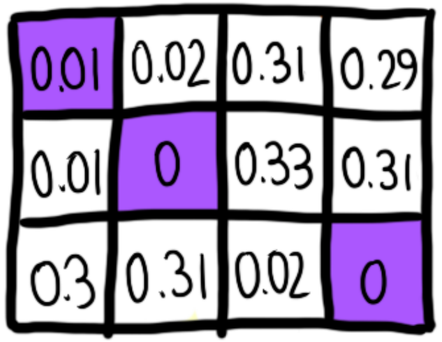
Linear Assignment Problem (LAP)

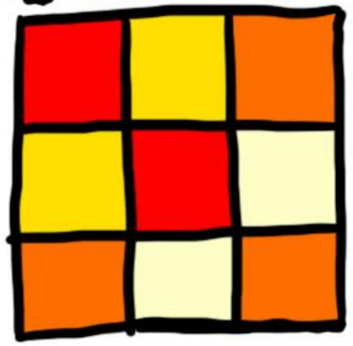
$\tilde{V}$ (n×n)



P (n×m)







V(m×m)

Hungarian algorithm

SAP [3]

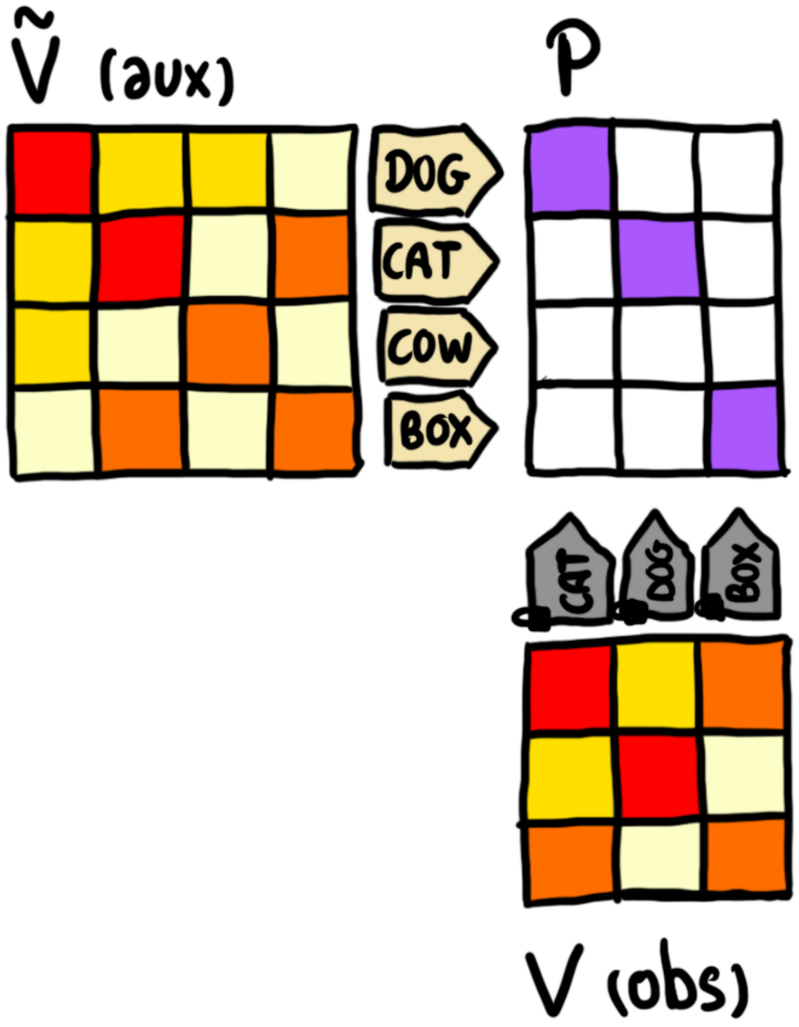
$$P = \underset{P \in \mathcal{P}}{\operatorname{argmin}} \sum_{i} \sum_{j} d_{ij} \cdot P_{ij}$$

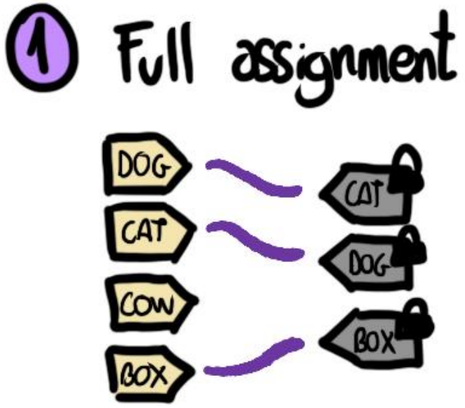
$O(n \cdot m + m^2 \cdot \log m)$

But lots of wasted information

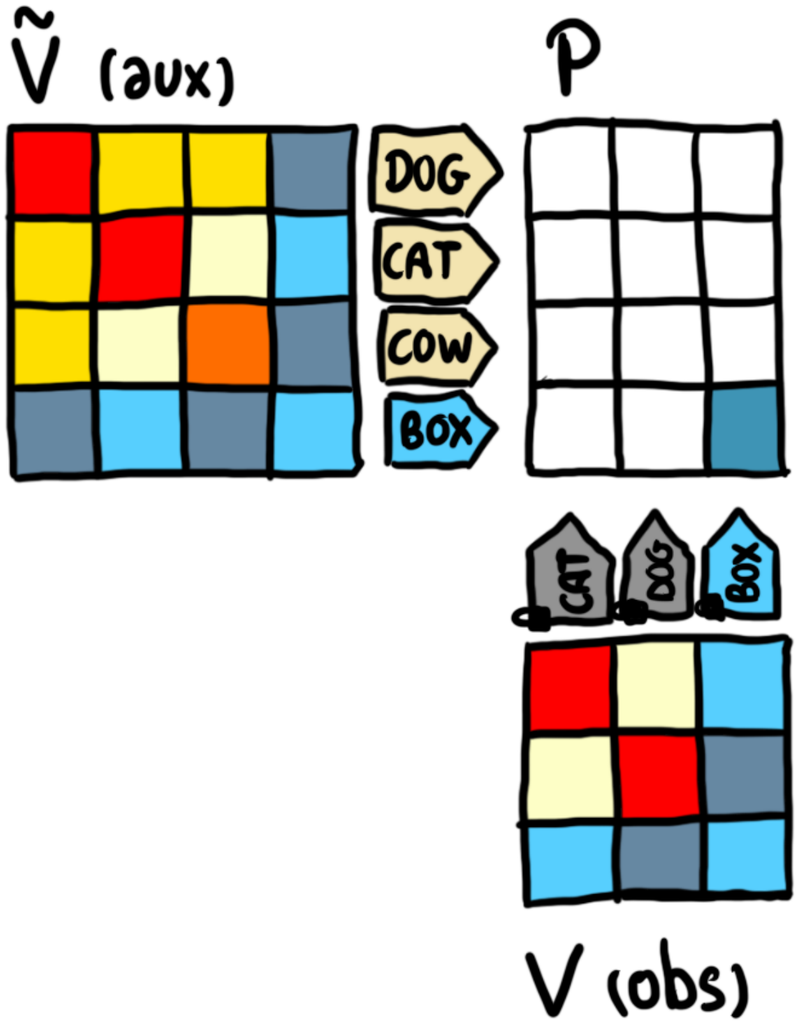
[3] Oya and Kerschbaum. *Hiding the access pattern is not enough: Exploiting search pattern leakage in searchable encryption.* USENIX 2021

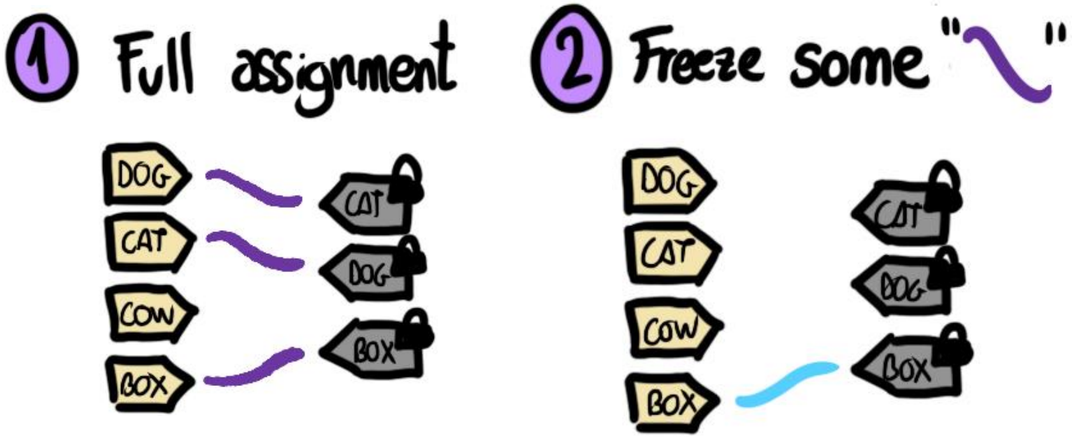
IHOP: Iteration Heuristic for (Quadratic) Optimization Problems



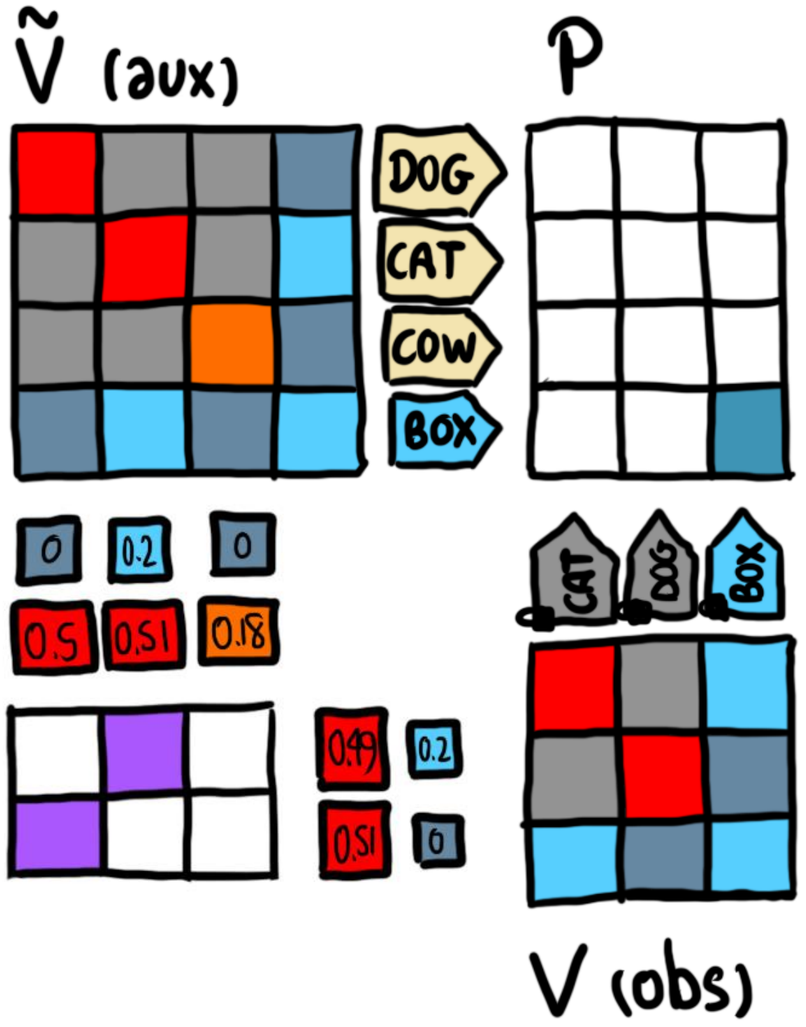


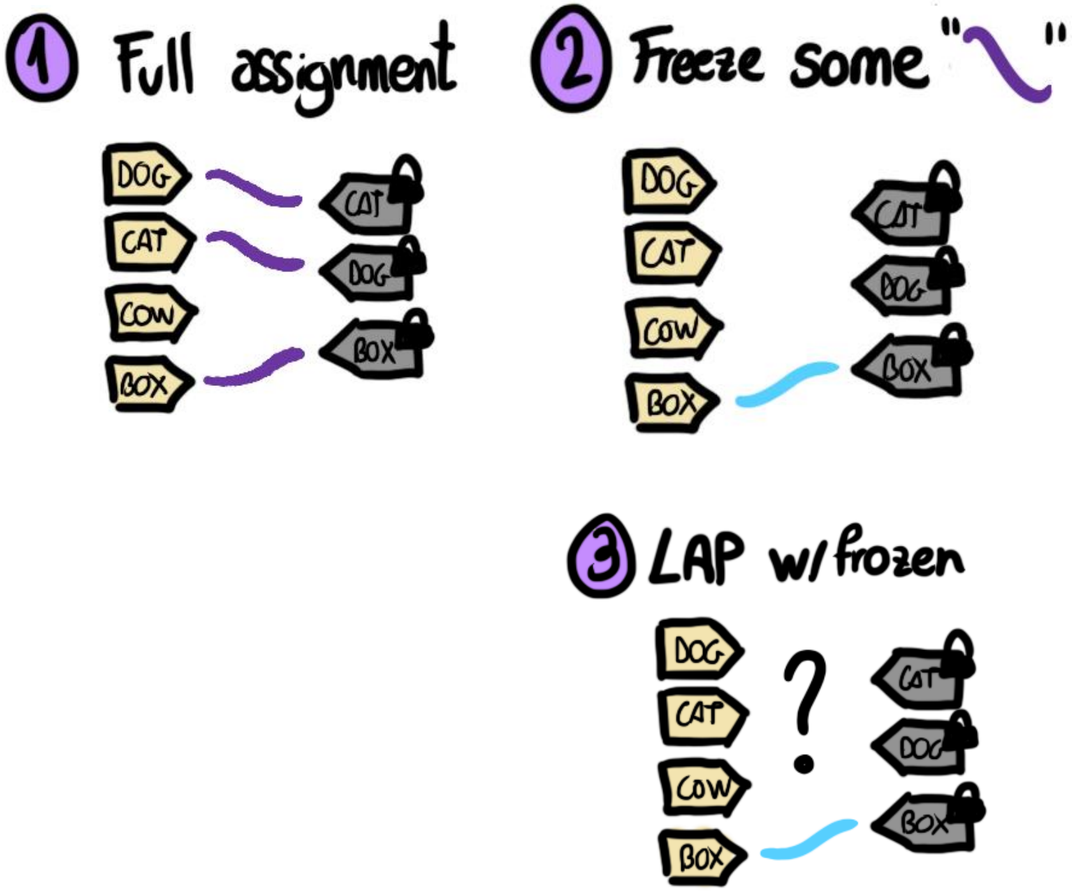
IHOP: Iteration Heuristic for (Quadratic) Optimization Problems



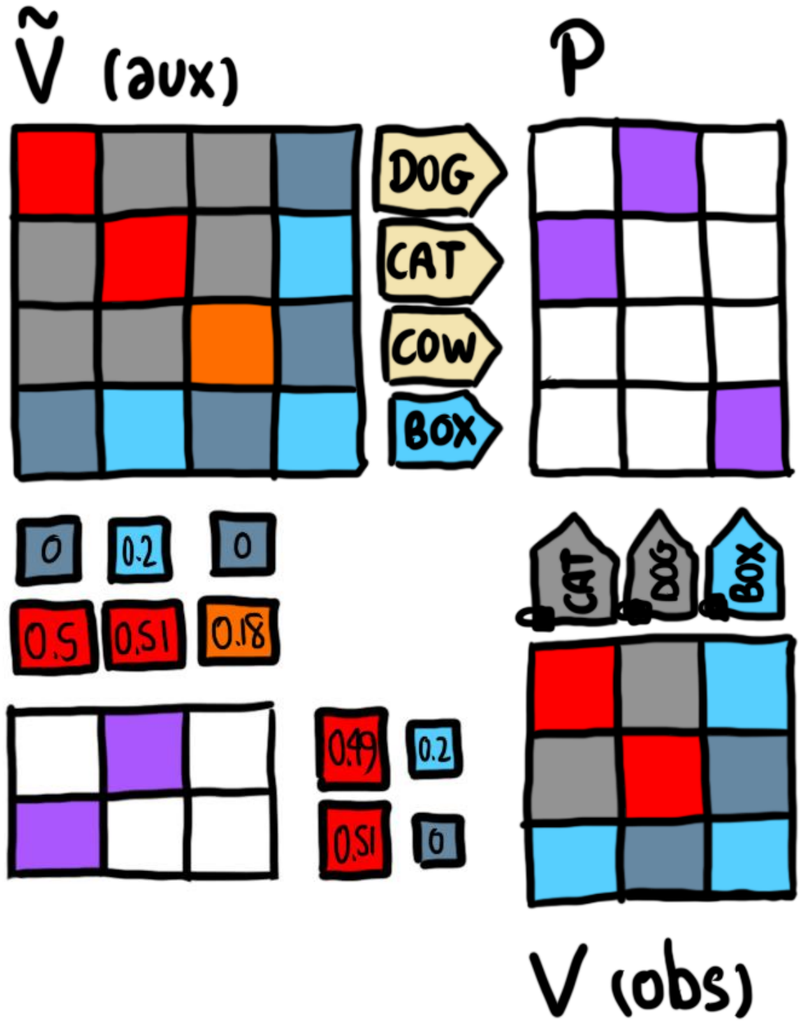


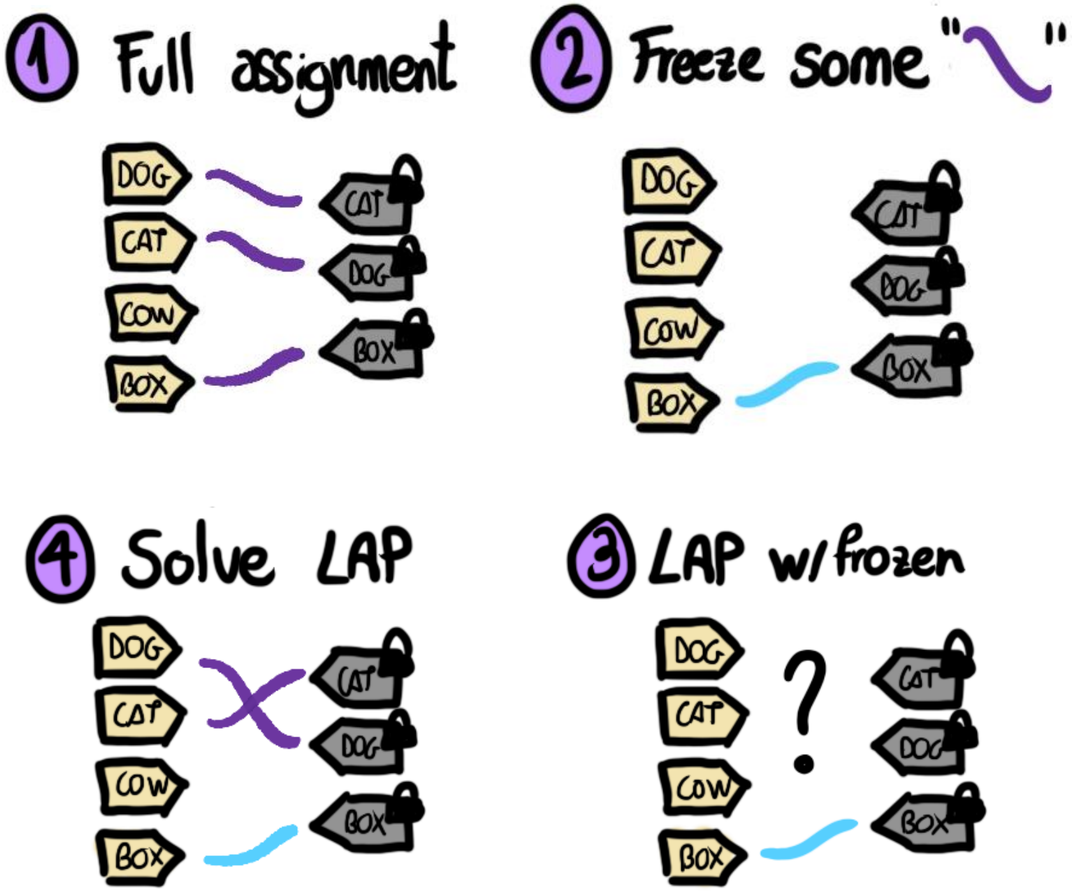
IHOP: Iteration Heuristic for (Quadratic) Optimization Problems



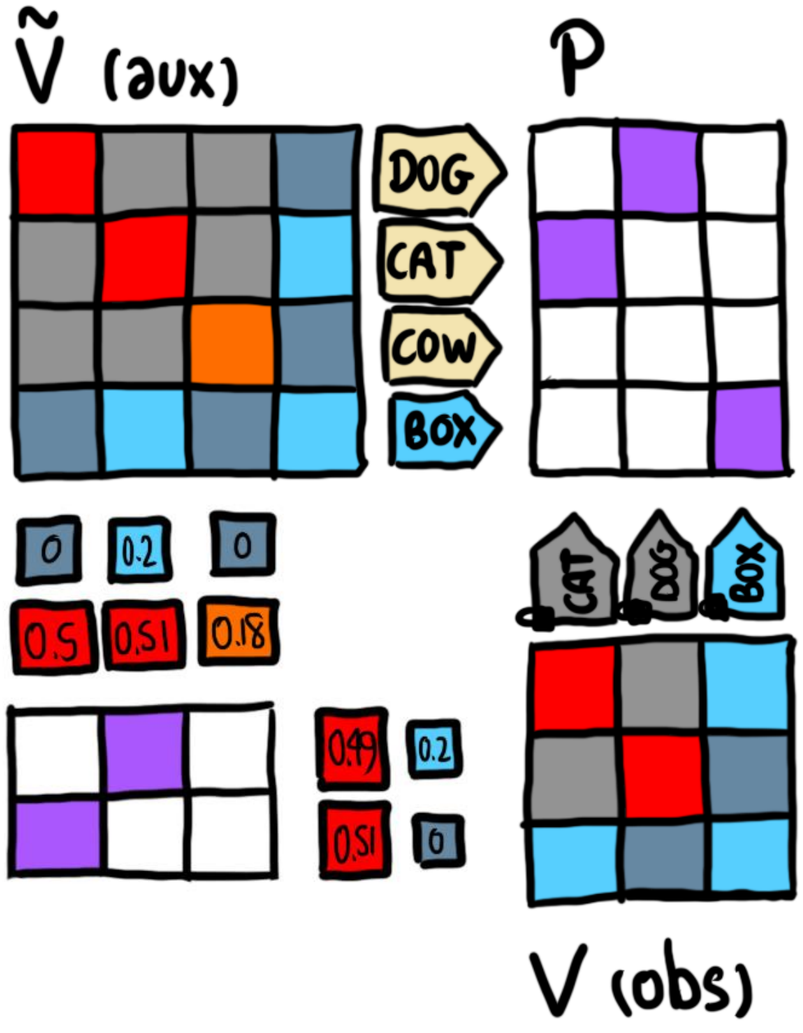


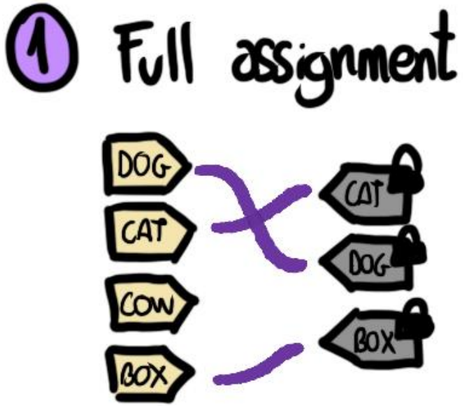
IHOP: Iteration Heuristic for (Quadratic) Optimization Problems

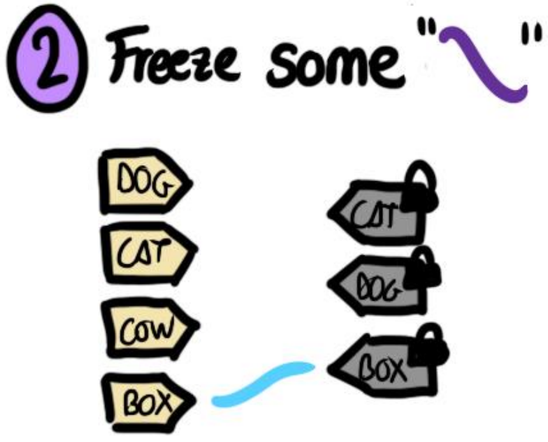


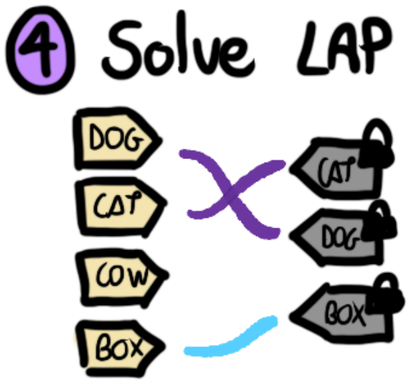


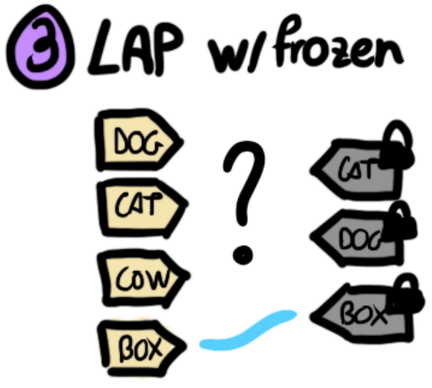
IHOP: Iteration Heuristic for (Quadratic) Optimization Problems





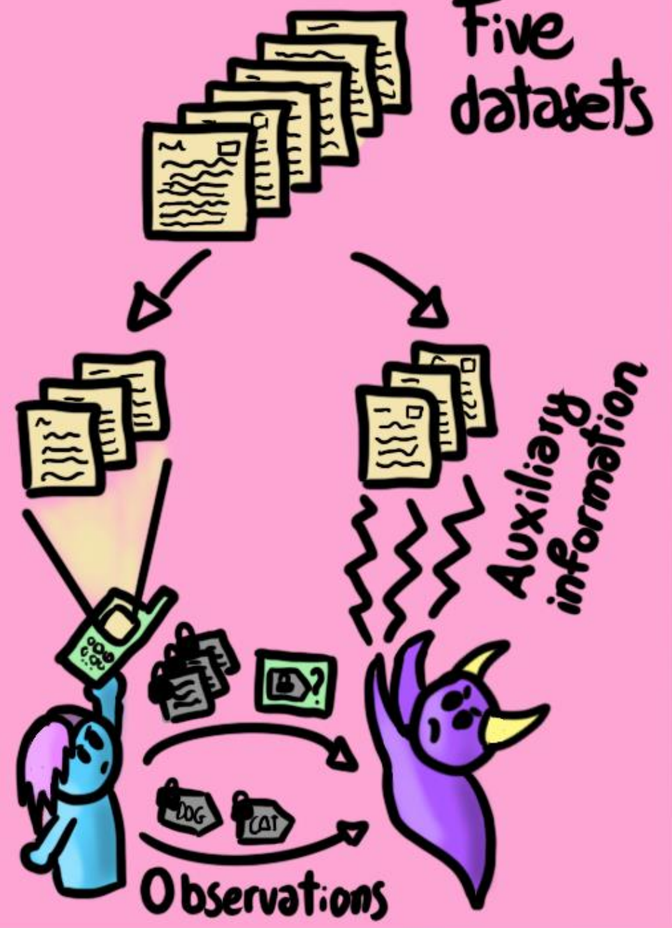




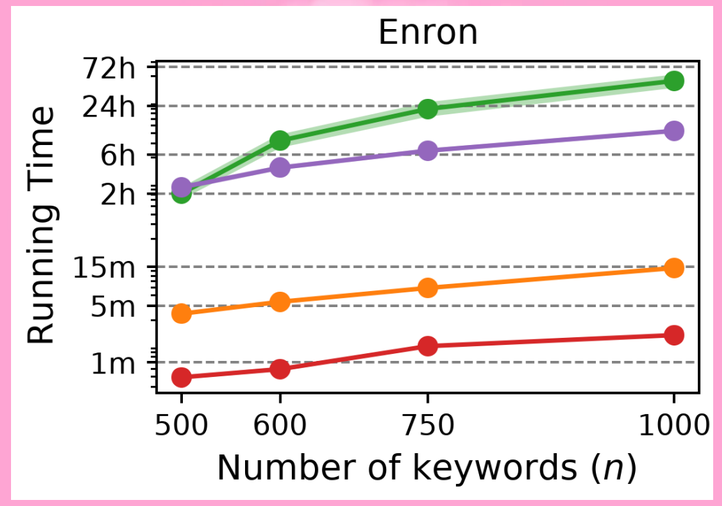


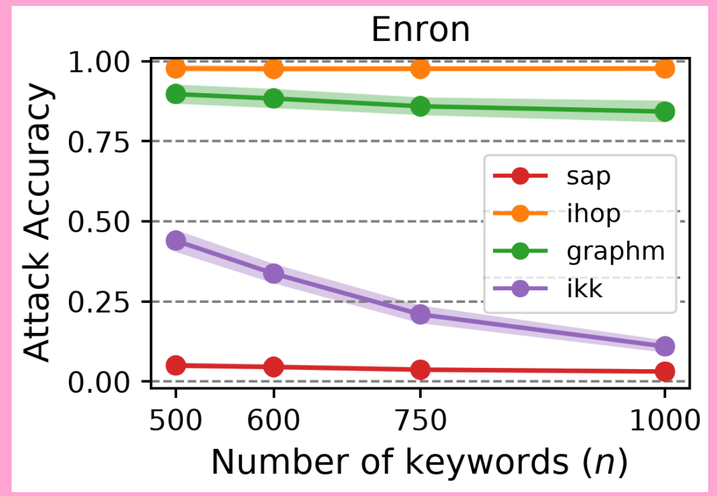
Some experiments

Setup

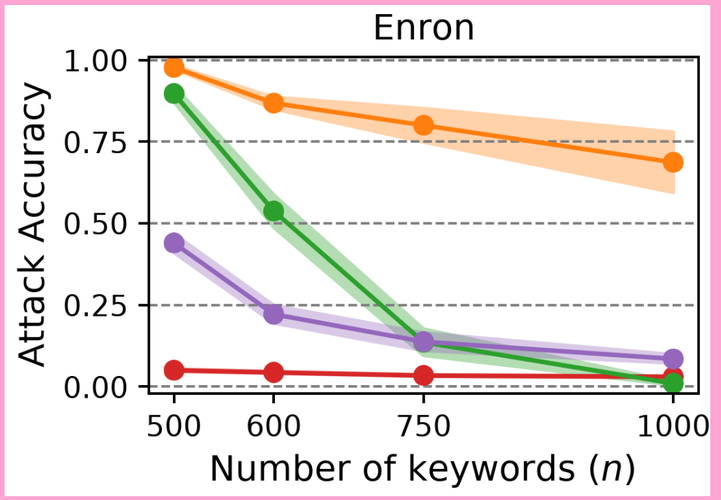


Attacks vs. # =

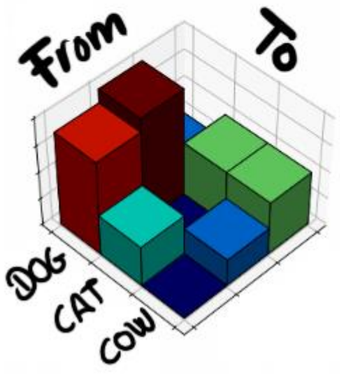


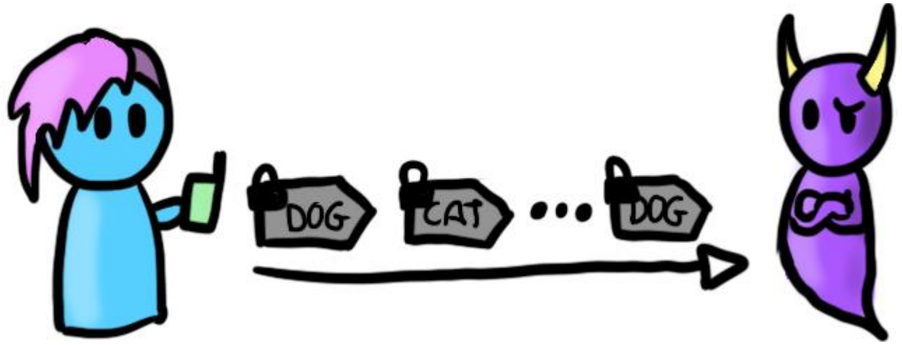


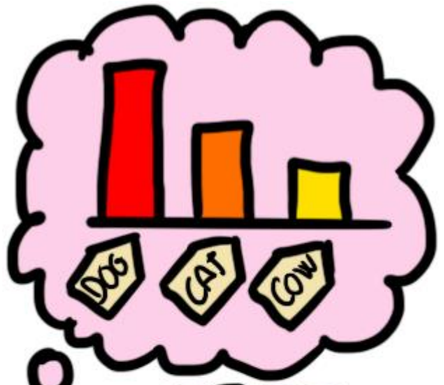
Attacks vs. # ≠

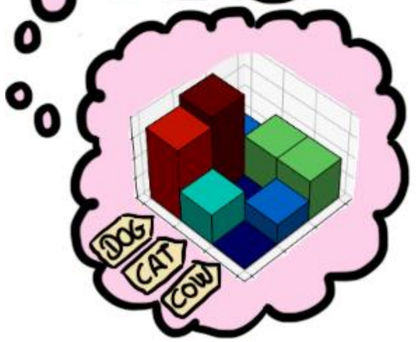


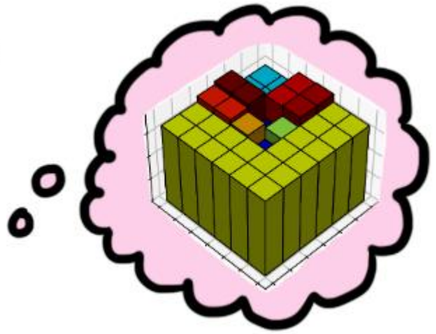
IHOP vs. Pancake (very briefly)

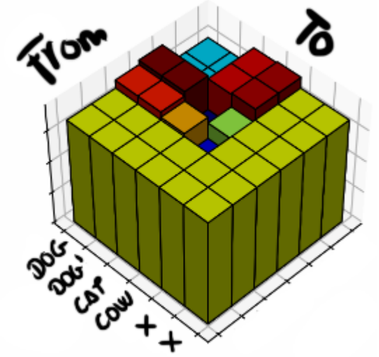


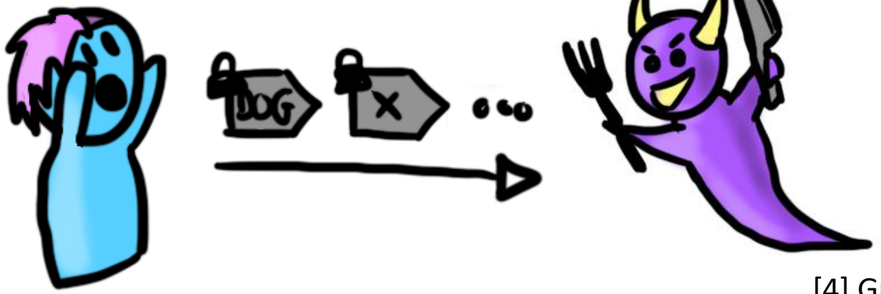












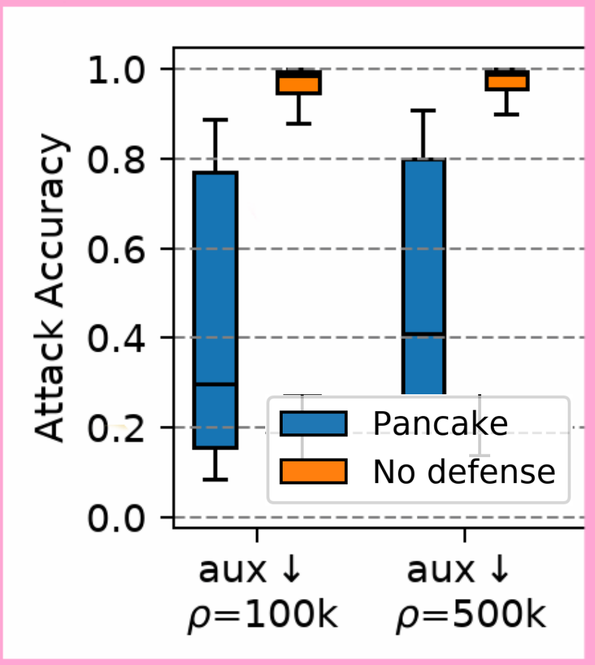
Some Results

Wikipedia Datasets

500 documents

↓

1000 replicas




IHOP
New!
Statistical Query Recovery Attack
FASTER!
MORE ACCURATE!
FLEXIBLE
Questions?
Simon.oya@uwaterloo.ca