Optimally Hiding Object Sizes with Constrained Padding

Andrew C. Reed
United States Military Academy
andrew.reed@westpoint.edu

Michael K. Reiter
Duke University
michael.reiter@duke.edu

36th IEEE Computer Security Foundations Symposium
July 13, 2023

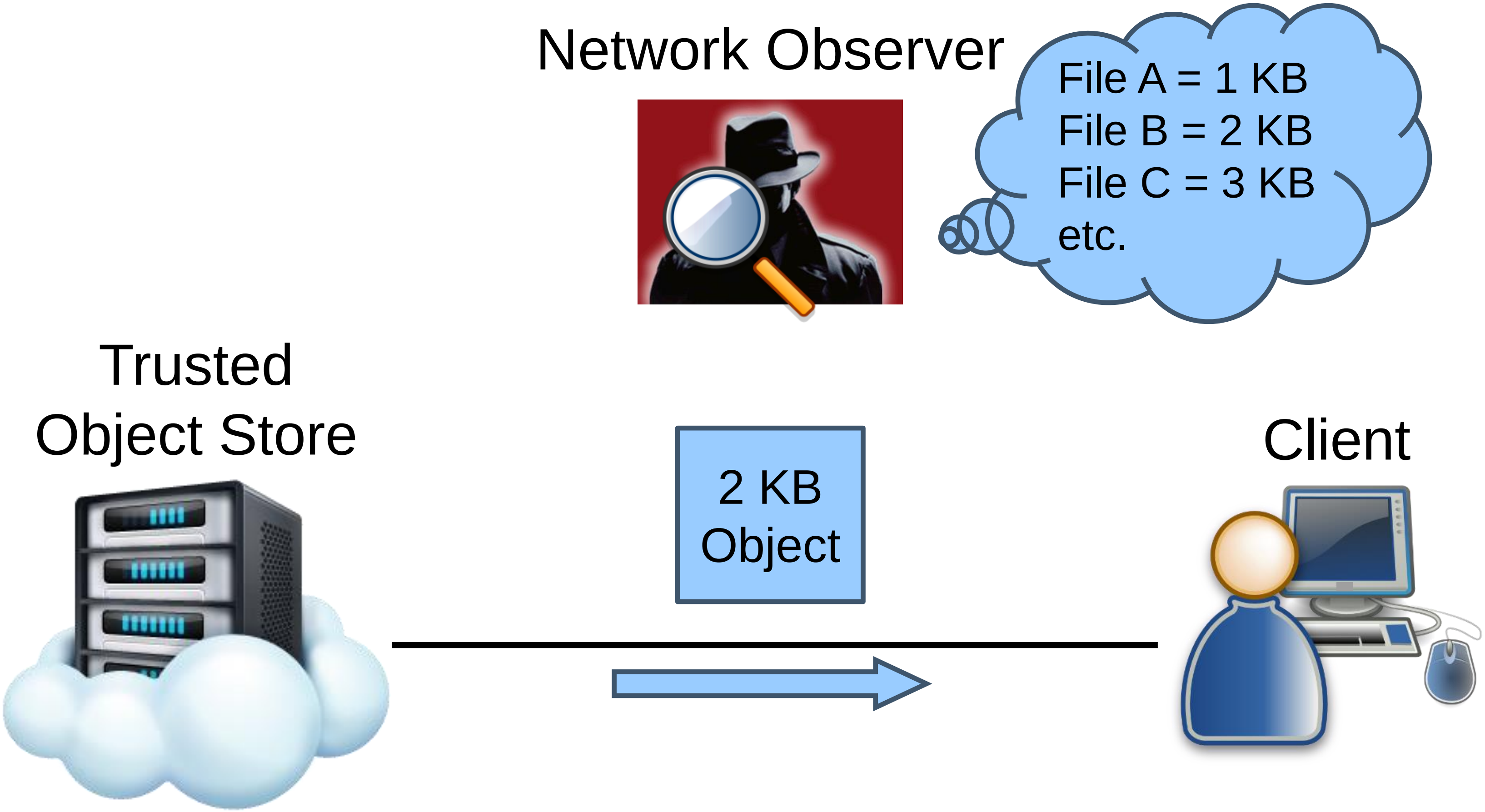
Agenda

- Objective
- Algorithms
- Evaluation
- Questions

Agenda

- Objective
- Algorithms
- Evaluation
- Questions

Objective: High Level



Network Observer

File A = 1 KB
File B = 2 KB
File C = 3 KB
etc.

Trusted
Object Store

2 KB
Object

Client

- **Client** has retrieved an object from **Trusted Object Store**
- **Network Observer’s** goal is to identify which object was requested

Objective: High Level

- Threat: A network observer with the following…
  - Capability: discern the sizes of retrieved objects
  - Goal: identify which object was retrieved
  - Knows:
    - every object’s size and how often requested
    - the padding defense used by object store
- Trusted Object Store’s Goals:
  1. Use padding to best thwart the adversary
  2. Control the overhead due to padding
  3. Address multiple scenarios

Objective: Formalized

- Objective:
  - Minimize I(S;Y) = H(S) – H(S|Y)
    - S = random variable for an object's **identity**
    - Y = random variable for an object's **padded size**
- Notation:
  - object *s* **original** size = $|\mathsf{obj}_s|$
  - object *s* **padded** size = $\lceil \mathsf{obj}_s \rceil$
- Constraints:
  - Objects are served in full

$$\mathbb{P}(\lceil \mathsf{obj}_s \rceil < |\mathsf{obj}_s|) = 0$$

  - Objects are not padded by more than a factor of *c*

$$\mathbb{P}(\lceil \mathsf{obj}_s \rceil > c \times |\mathsf{obj}_s|) = 0$$

Note: it's possible for some objects to remain isolated in our setting

Objective: Add’l Considerations

- Key Assumption:
  - Independent object retrievals

- Scenarios Addressed:
  - Per-Object Padding
  - Per-Request Padding
  - Unknown Query Distribution

Agenda

- Objective
- Algorithms
- Evaluation
- Questions

Algorithms: Overview

- Inputs:
  - S = distribution for object queries
  - *c* = max padding factor per object

- Output:
  - A padding scheme $\lceil \cdot \rceil$ that minimizes I(S;Y)* and does not violate *c* for any object

* for the given scenario

Per-Object Padding

- Setting:
  - Each object is padded only once
- Key Insights:
  - $I(S;Y) = H(S) - H(S|Y) = H(Y) - \cancelto{0}{H(Y|S)}$
    - Sufficient to minimize H(Y)
  - Optimal $\lceil \cdot \rceil$ will be a partition of contiguous blocks

e.g., for *c* = 1.05 and original object sizes:	100	105	109	110	113	114	115
Optimal $\lceil \cdot \rceil$ **will not** be of the form:	105	105	114	115	115	114	115
Optimal $\lceil \cdot \rceil$ **will** be of the form:	105	105	114	114	114	114	115

- Solution:
  - Dynamic programming algorithm that runs in $O((\#S)^2)$

Per-Request Padding

- Setting:
  - Objects are padded anew with each request
- Key Insight:
  - Special case of *rate-distortion minimization*[1]
- Solution:
  - Use the iterative algorithm "Blahut-Arimoto"[2,3] with:
    - $D(s,y) = 0$ If s can be padded to y
    - $D(s,y) = \infty$ If s cannot be padded to y

[1] C. E. Shannon, "Coding theorems for a discrete source with a fidelity criterion," in *Institute of Radio Engineers, International Convention Record*, vol. 7, 1959.

[2] R. Blahut, "Computation of channel capacity and rate-distortion functions," *IEEE Transactions on Information Theory*, vol. 18, no. 4, Jul. 1972.

[3] S. Arimoto, "An algorithm for computing the capacity of arbitrary discrete memoryless channels," *IEEE Transactions on Information Theory*, vol. 18, no. 1, Jan. 1972.

Unknown Query Distribution

- Setting:
  - The object store does not know (or is not confident in) the distribution S
- Key Insights:
  - Minimize Sibson mutual information of order infinity: $I_\infty(S;Y)$
    - Advocated by multiple researchers as a privacy metric[4,5]
  - $I(S;Y) \leq I_\infty(S;Y)$
  - $I_\infty(S;Y)$ only requires that the object store know which objects have a nonzero probability of being retrieved
- Solution:
  - A greedy algorithm that runs in time linear in #S

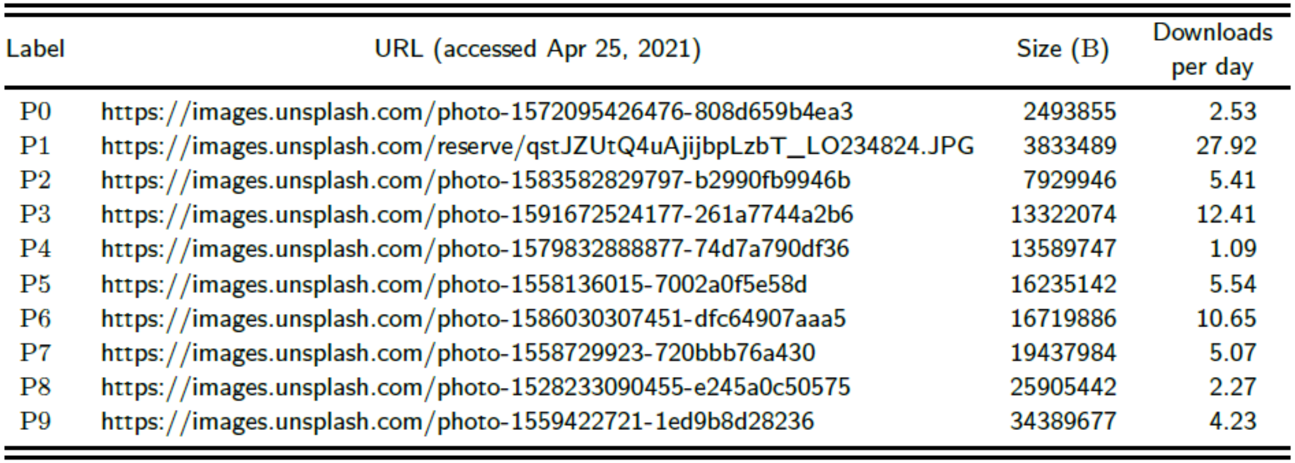
[4] M. Alvim, K. Chatzikokolakis, C. Palamidessi, and G. Smith, "Measuring information leakage using generalized gain functions," in *25th IEEE Computer Security Foundations*, Jun. 2012.

[5] I. Issa, A. B. Wagner, and S. Kamath, "An operational approach to information leakage," *IEEE Transactions on Information Theory*, vol. 66, no. 3, Mar. 2020.

Example Padding Schemes

Inputs:

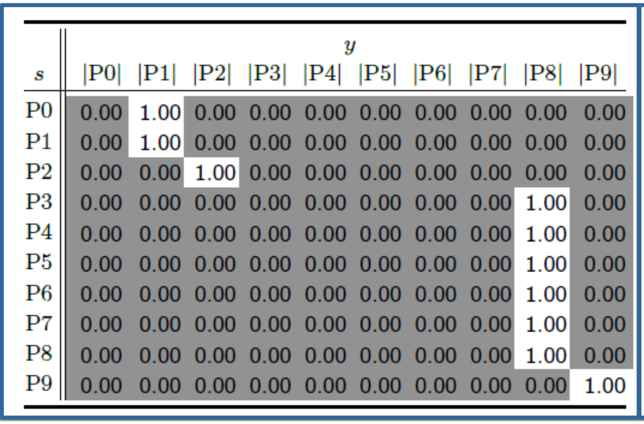
c = 2 &



Label	URL (accessed Apr 25, 2021)	Size (B)	Downloads per day
P0	https://images.unsplash.com/photo-1572095426476-808d659b4ea3	2493855	2.53
P1	https://images.unsplash.com/reserve/qstJZUtQ4uAjijbpLzbT_LO234824.JPG	3833489	27.92
P2	https://images.unsplash.com/photo-1583582829797-b2990fb9946b	7929946	5.41
P3	https://images.unsplash.com/photo-1591672524177-261a7744a2b6	13322074	12.41
P4	https://images.unsplash.com/photo-1579832888877-74d7a790df36	13589747	1.09
P5	https://images.unsplash.com/photo-1558136015-7002a0f5e58d	16235142	5.54
P6	https://images.unsplash.com/photo-1586030307451-dfc64907aaa5	16719886	10.65
P7	https://images.unsplash.com/photo-1558729923-720bbb76a430	19437984	5.07
P8	https://images.unsplash.com/photo-1528233090455-e245a0c50575	25905442	2.27
P9	https://images.unsplash.com/photo-1559422721-1ed9b8d28236	34389677	4.23

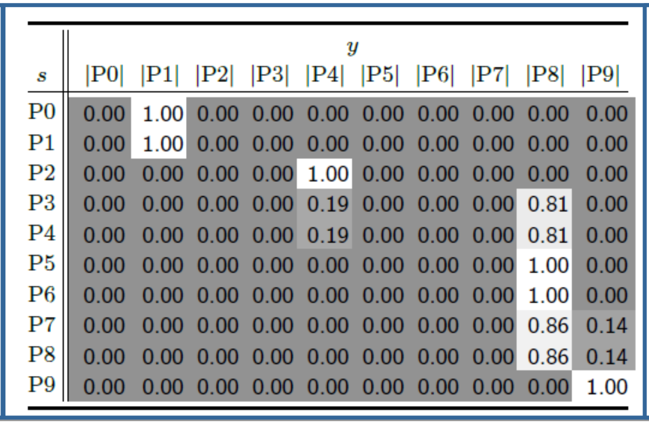
Outputs:

Per-Object



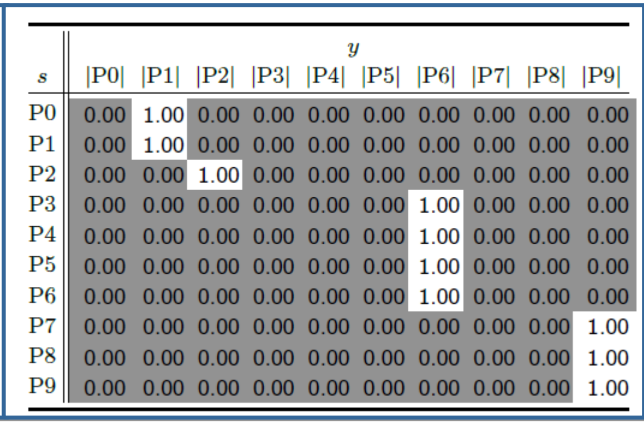
	y									
s	|P0|	|P1|	|P2|	|P3|	|P4|	|P5|	|P6|	|P7|	|P8|	|P9|
P0	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P1	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P2	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00
P4	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00
P5	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00
P6	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00
P7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00
P8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00
P9	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00

Per-Request



	y									
s	|P0|	|P1|	|P2|	|P3|	|P4|	|P5|	|P6|	|P7|	|P8|	|P9|
P0	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P1	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P2	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00
P3	0.00	0.00	0.00	0.00	0.19	0.00	0.00	0.00	0.81	0.00
P4	0.00	0.00	0.00	0.00	0.19	0.00	0.00	0.00	0.81	0.00
P5	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00
P6	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00
P7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.86	0.14
P8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.86	0.14
P9	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00

Unknown Dist.



	y									
s	|P0|	|P1|	|P2|	|P3|	|P4|	|P5|	|P6|	|P7|	|P8|	|P9|
P0	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P1	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P2	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P3	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00
P4	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00
P5	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00
P6	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00
P7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00
P8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00
P9	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00

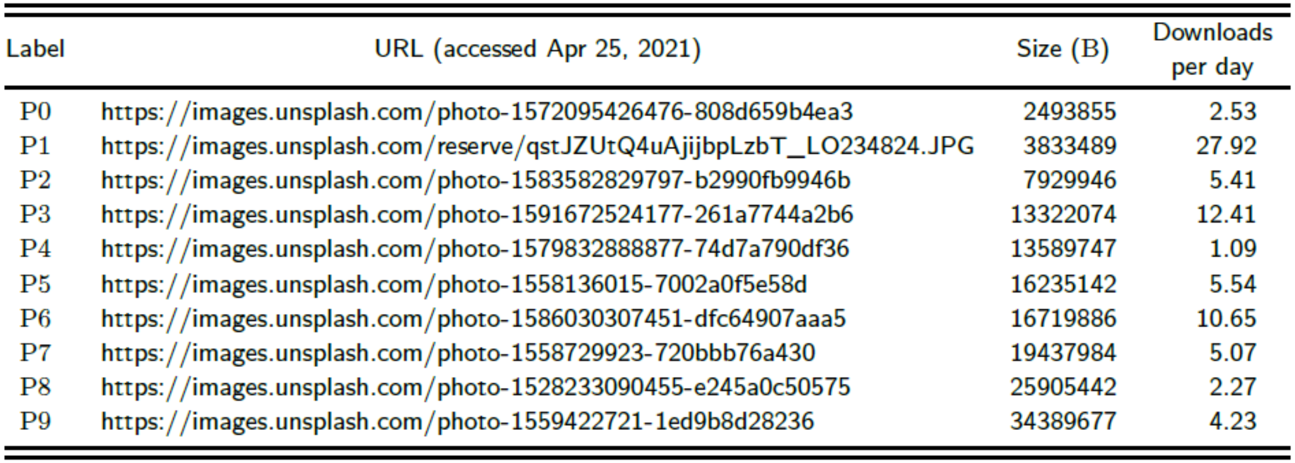
Agenda

- Objective
- Algorithms
- Evaluation
- Questions

Competitors

Inputs:

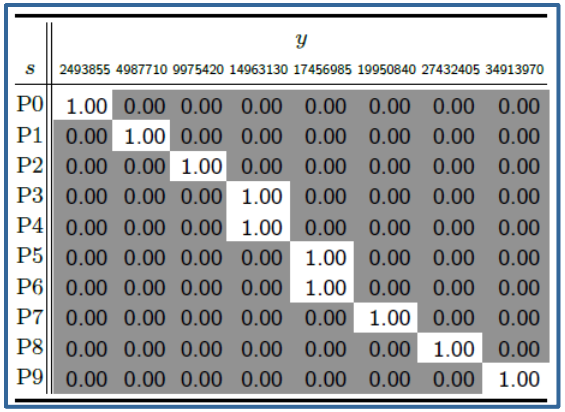
$c = 2$ &



Label	URL (accessed Apr 25, 2021)	Size (B)	Downloads per day
P0	https://images.unsplash.com/photo-1572095426476-808d659b4ea3	2493855	2.53
P1	https://images.unsplash.com/reserve/qstJZUtQ4uAjijbpLzbT_LO234824.JPG	3833489	27.92
P2	https://images.unsplash.com/photo-1583582829797-b2990fb9946b	7929946	5.41
P3	https://images.unsplash.com/photo-1591672524177-261a7744a2b6	13322074	12.41
P4	https://images.unsplash.com/photo-1579832888877-74d7a790df36	13589747	1.09
P5	https://images.unsplash.com/photo-1558136015-7002a0f5e58d	16235142	5.54
P6	https://images.unsplash.com/photo-1586030307451-dfc64907aaa5	16719886	10.65
P7	https://images.unsplash.com/photo-1558729923-720bbb76a430	19437984	5.07
P8	https://images.unsplash.com/photo-1528233090455-e245a0c50575	25905442	2.27
P9	https://images.unsplash.com/photo-1559422721-1ed9b8d28236	34389677	4.23

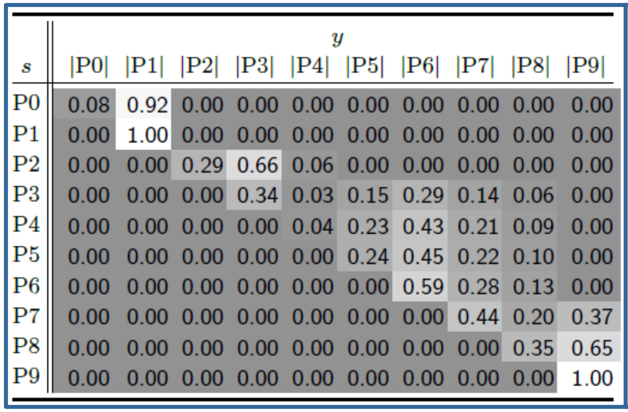
Outputs:

D-ALPaCA[6]



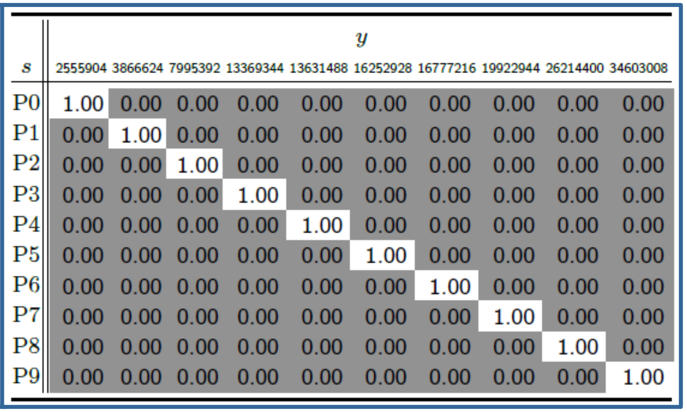
	y							
s	2493855	4987710	9975420	14963130	17456985	19950840	27432405	34913970
P0	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P1	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00
P2	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00
P3	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00
P4	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00
P5	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00
P6	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00
P7	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00
P8	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00
P9	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00

P-ALPaCA[6]



	y									
s	|P0|	|P1|	|P2|	|P3|	|P4|	|P5|	|P6|	|P7|	|P8|	|P9|
P0	0.08	0.92	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P1	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P2	0.00	0.00	0.29	0.66	0.06	0.00	0.00	0.00	0.00	0.00
P3	0.00	0.00	0.00	0.34	0.03	0.15	0.29	0.14	0.06	0.00
P4	0.00	0.00	0.00	0.00	0.04	0.23	0.43	0.21	0.09	0.00
P5	0.00	0.00	0.00	0.00	0.00	0.24	0.45	0.22	0.10	0.00
P6	0.00	0.00	0.00	0.00	0.00	0.00	0.59	0.28	0.13	0.00
P7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.44	0.20	0.37
P8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.35	0.65
P9	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00

Padmé[7]

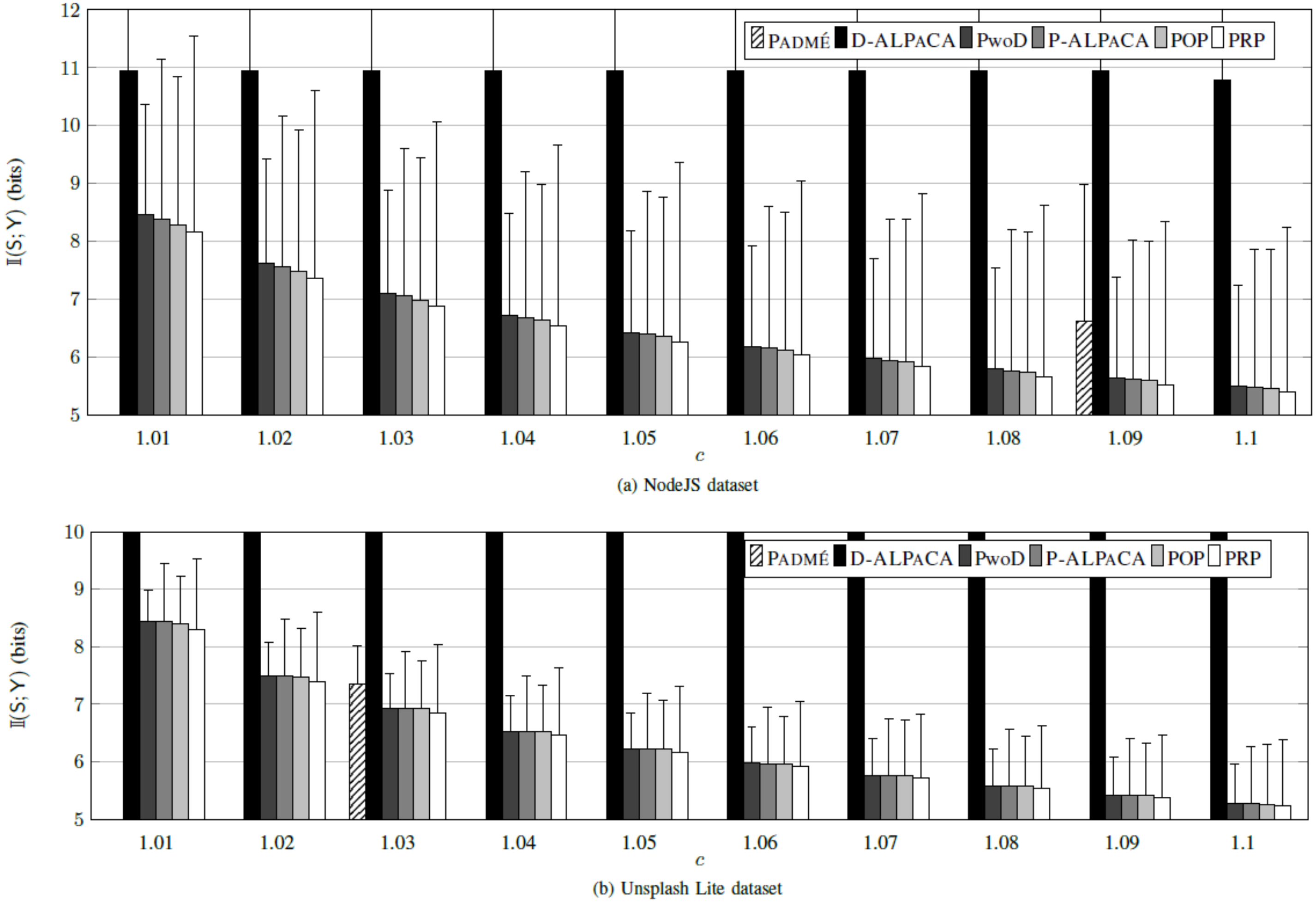


	y									
s	2555904	3866624	7995392	13369344	13631488	16252928	16777216	19922944	26214400	34603008
P0	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P1	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P2	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P3	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00
P4	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00
P5	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00
P6	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00
P7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00
P8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00
P9	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00

[6] G. Cherubin, J. Hayes, and M. Juarez, "Website fingerprinting defenses at the application layer," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 2, 2017.

[7] K. Nikitin, L. Barman, W. Lueks, M. Underwood, J.-P. Hubaux, and B. Ford, "Reducing metadata leakage from encrypted files and communication with PURBs," *Proceedings on Privacy Enhancing Technologies*, vol. 2019, no. 4, 2019.

Evaluation: Mutual Information

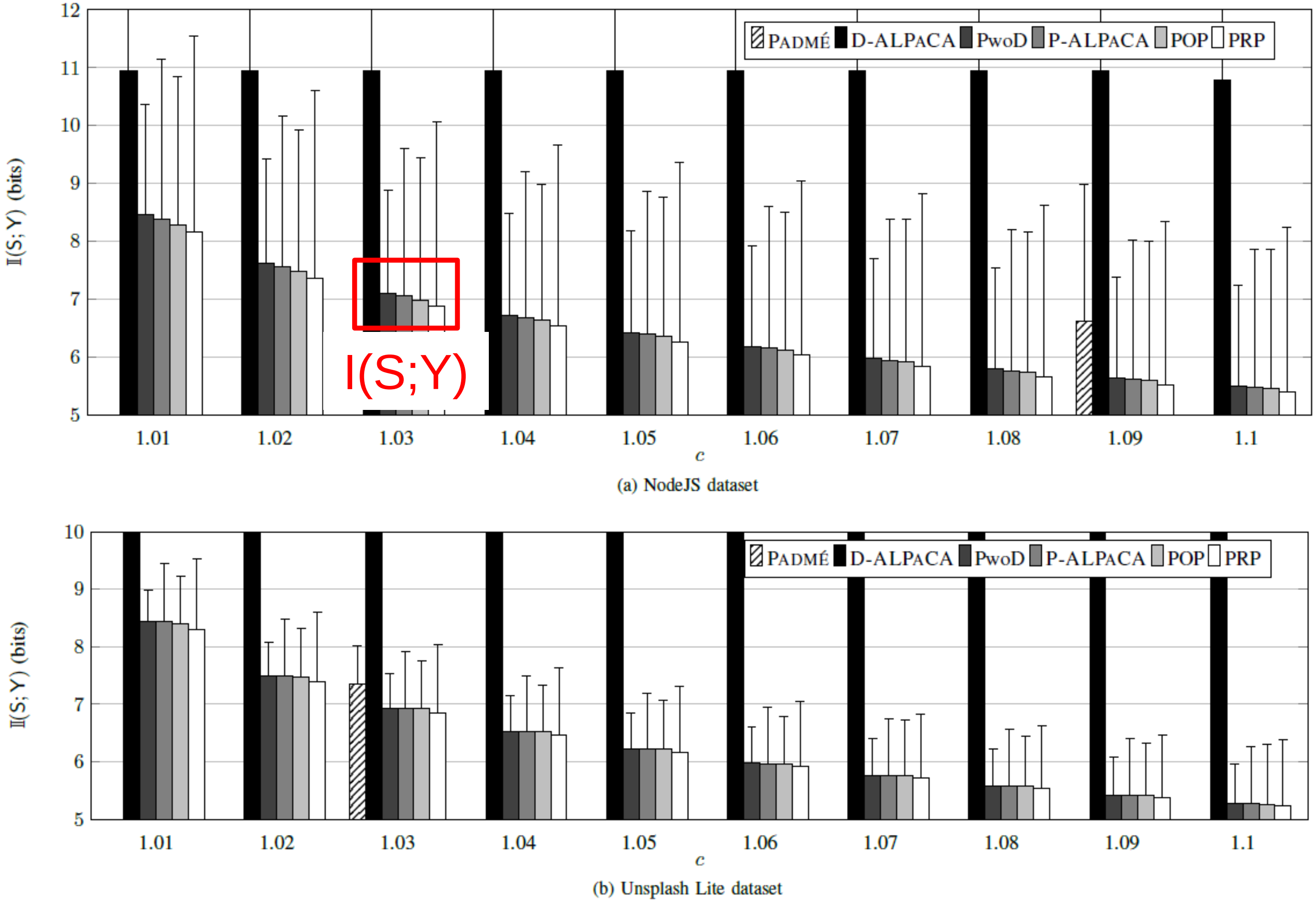


(a) NodeJS dataset

(b) Unsplash Lite dataset

Fig. 7: Per-algorithm mutual information. Error bars extend to $\mathbb{I}_\infty(S; Y)$. Lower values indicate better security.

Evaluation: Mutual Information



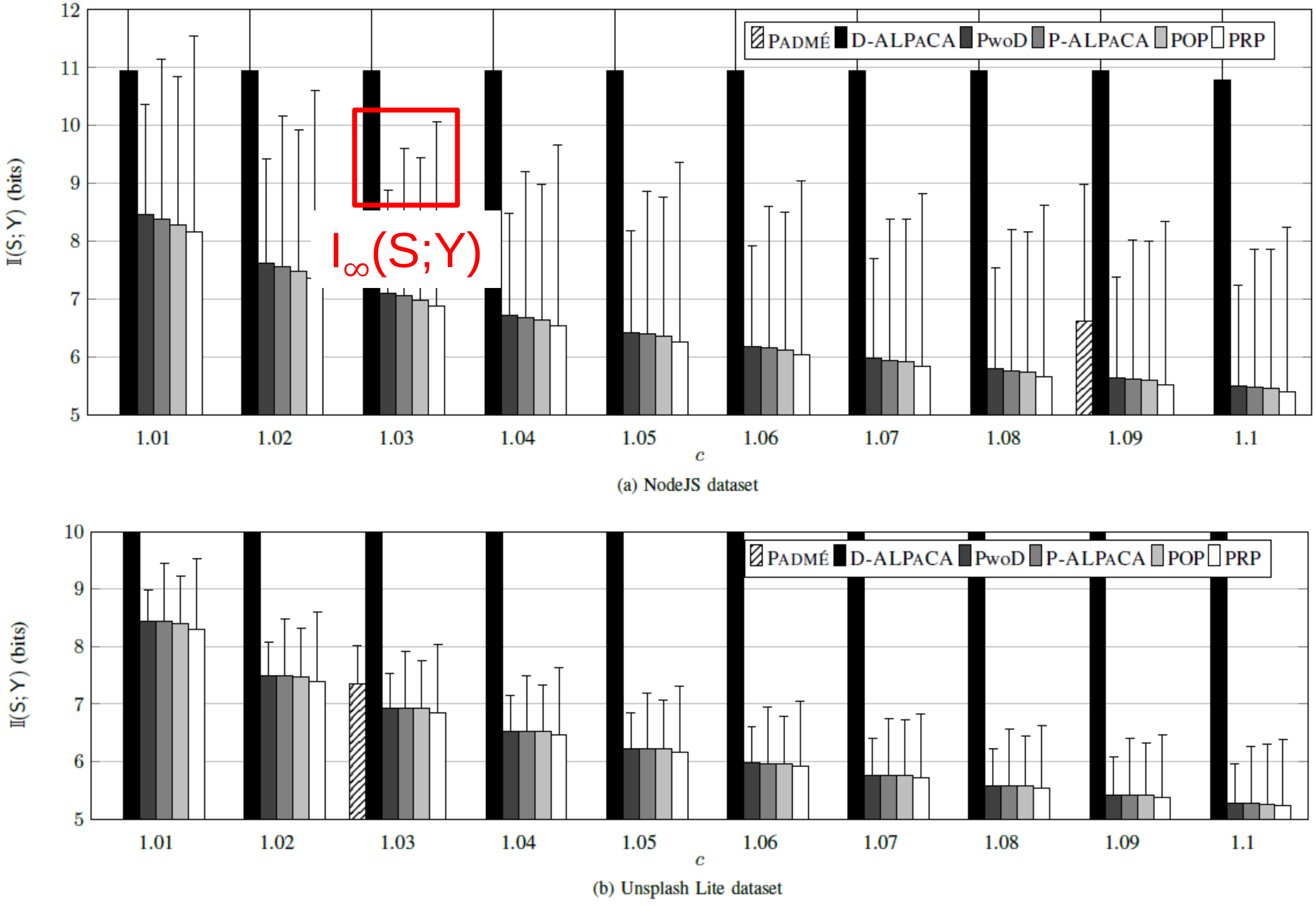
I(S;Y)

(a) NodeJS dataset

(b) Unsplash Lite dataset

Fig. 7: Per-algorithm mutual information. Error bars extend to $\mathbb{I}_\infty(S;Y)$. Lower values indicate better security.

Evaluation: Mutual Information

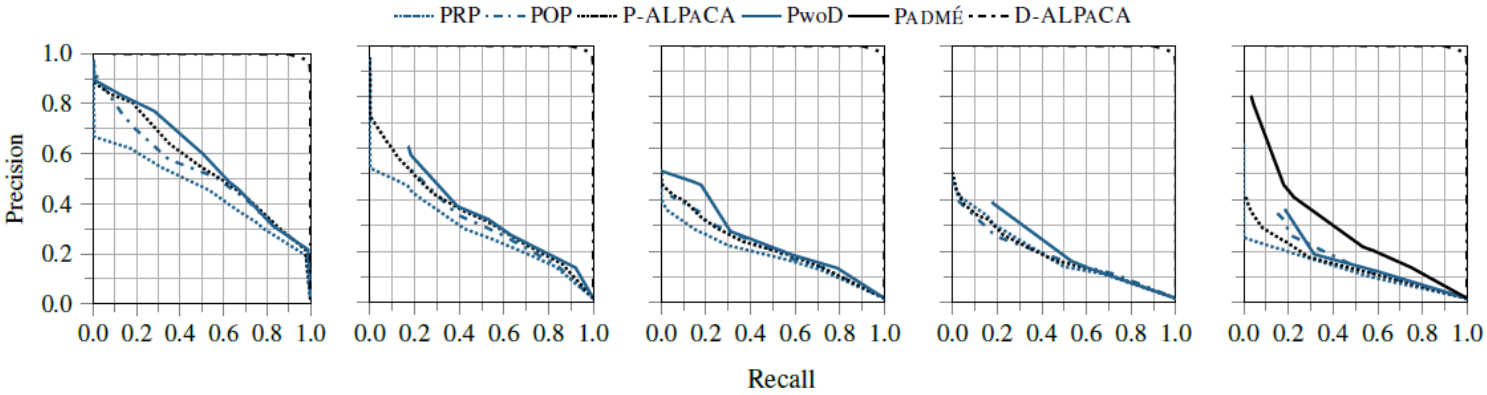


(a) NodeJS dataset

(b) Unsplash Lite dataset

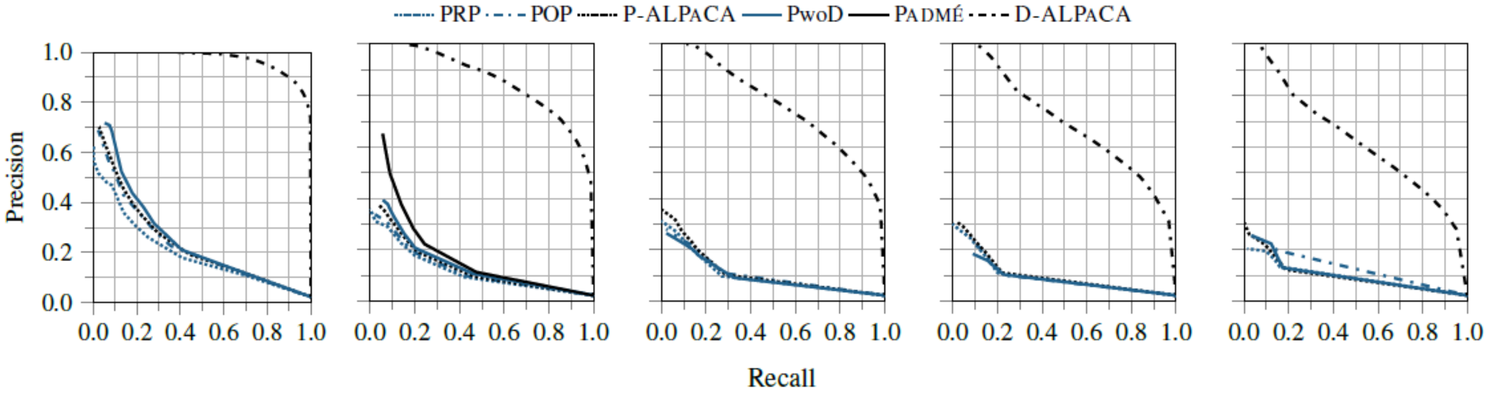
Fig. 7: Per-algorithm mutual information. Error bars extend to $\mathbb{I}_\infty(S; Y)$. Lower values indicate better security.

Evaluation: Recall & Precision



(a) $c = 1.01$ (b) $c = 1.03$ (c) $c = 1.05$ (d) $c = 1.07$ (e) $c = 1.09$

Fig. 8: Adversary's recall and precision for detecting vulnerable NodeJS packages.



(a) $c = 1.01$ (b) $c = 1.03$ (c) $c = 1.05$ (d) $c = 1.07$ (e) $c = 1.09$

Fig. 9: Adversary's recall and precision for detecting the Unsplash Lite *Nature* collection.

Evaluation: Runtimes

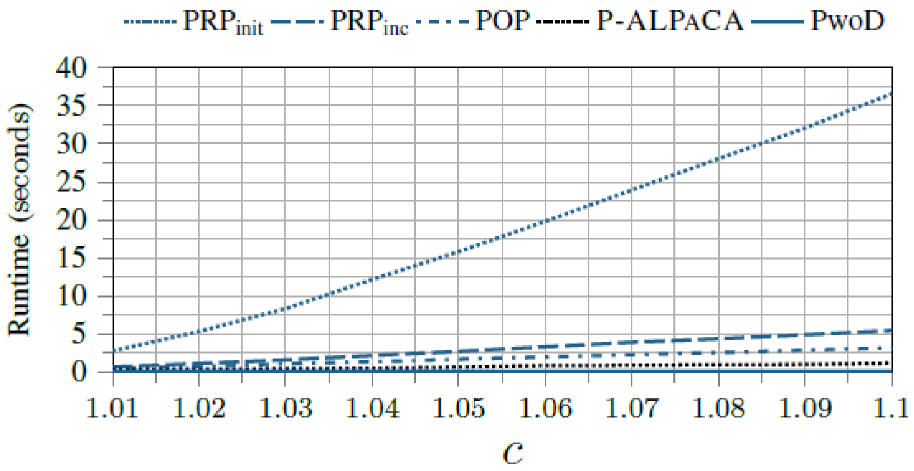


Fig. 12: Runtimes on the NodeJS dataset.

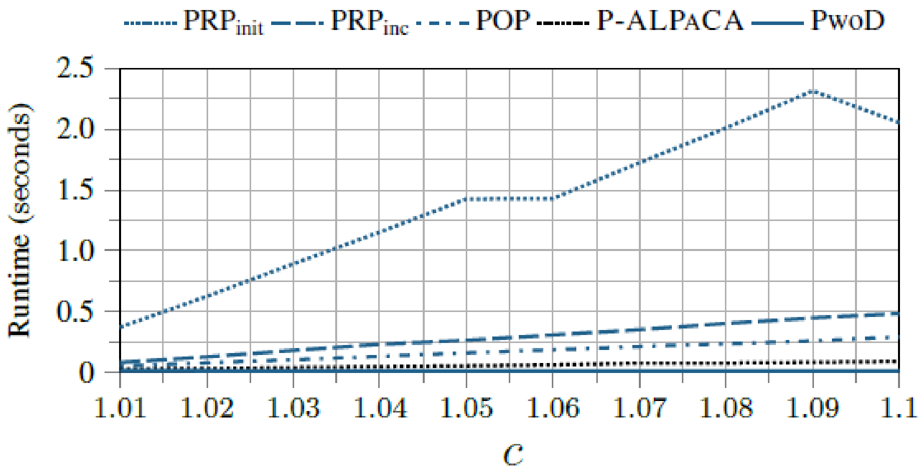


Fig. 13: Runtimes on the Unsplash Lite dataset.

Questions?