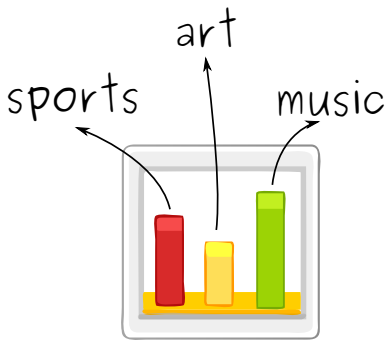
OB-PWS: Obfuscation-Based Private Web Search

Ero Balsa, Carmela Troncoso and Claudia Diaz

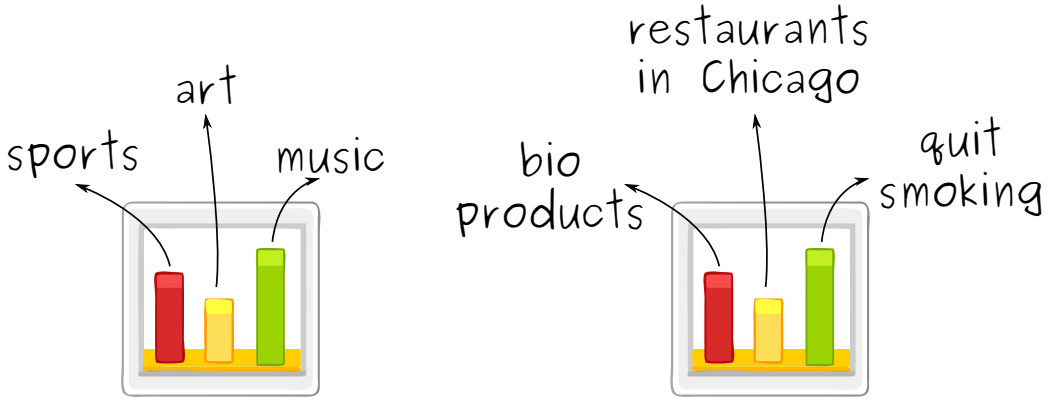
ESAT/COSIC, IBBT - KU Leuven

Wednesday, 23 May 2012

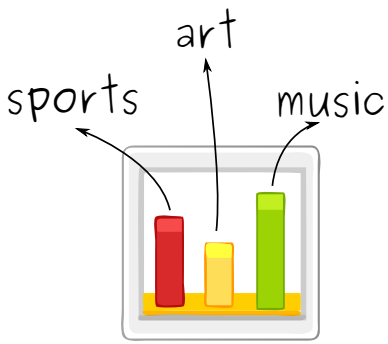
The Privacy Problem

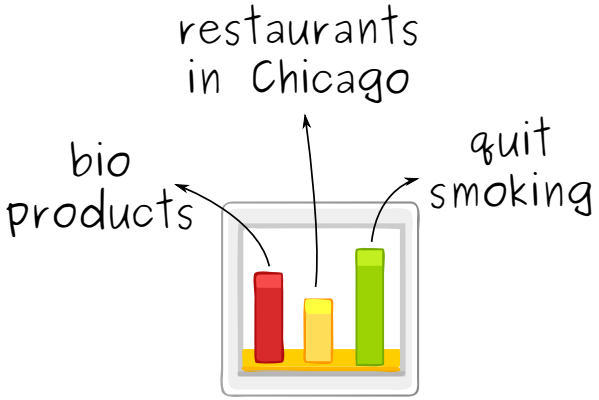


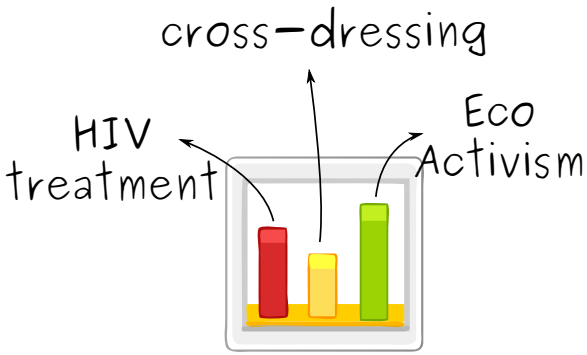
The Privacy Problem



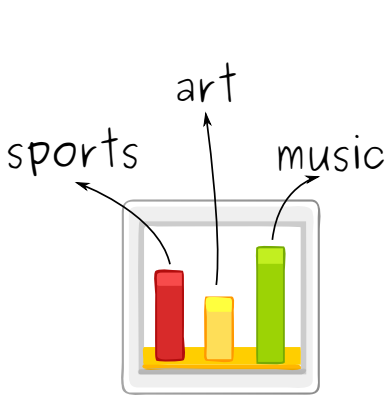
The Privacy Problem

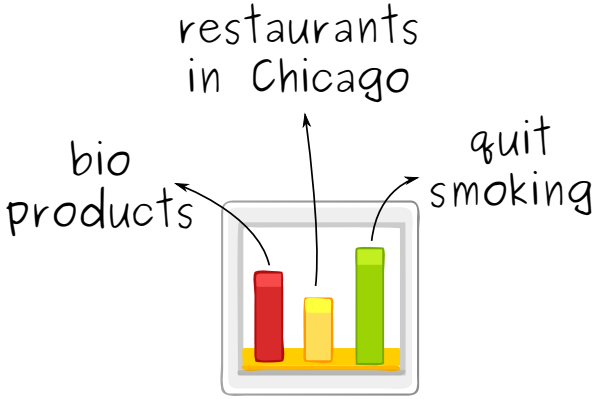


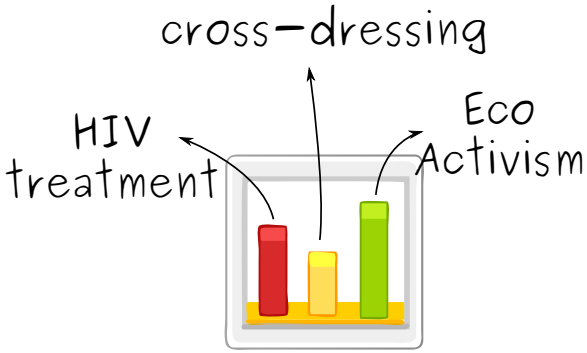




The Privacy Problem

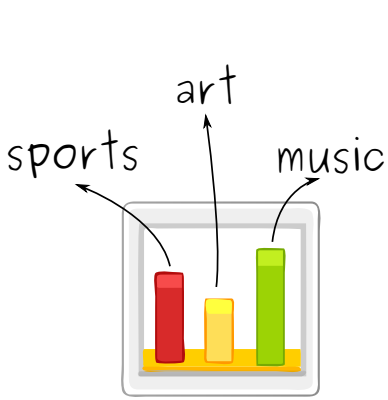


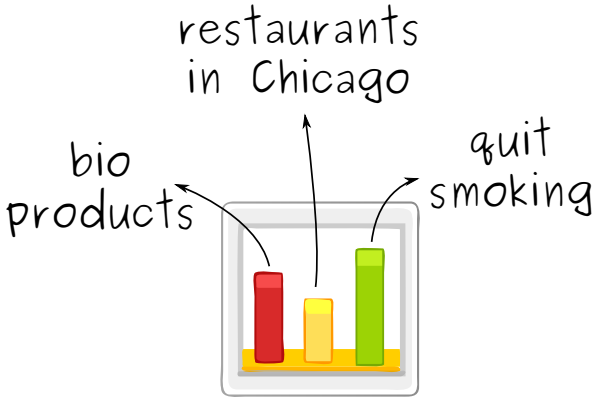


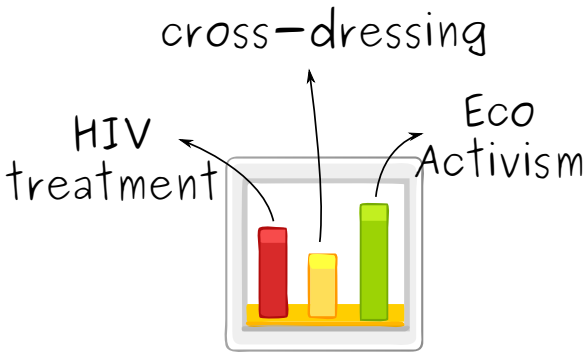


- PRIVACY PROBLEM:
  Individual search queries and/or profiling may reveal sensitive information.

The Privacy Problem





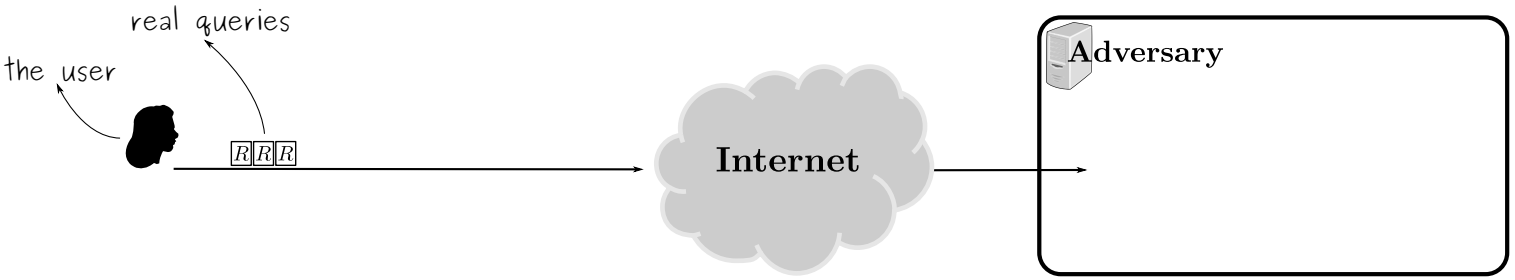


- PRIVACY PROBLEM:
  Individual search queries and/or profiling may reveal sensitive information.
- Some solutions:
  - Anonymous communications
  - PIR
  - **OB-PWS** $\Rightarrow$ Prevent **profiling** and provide query **deniability**.

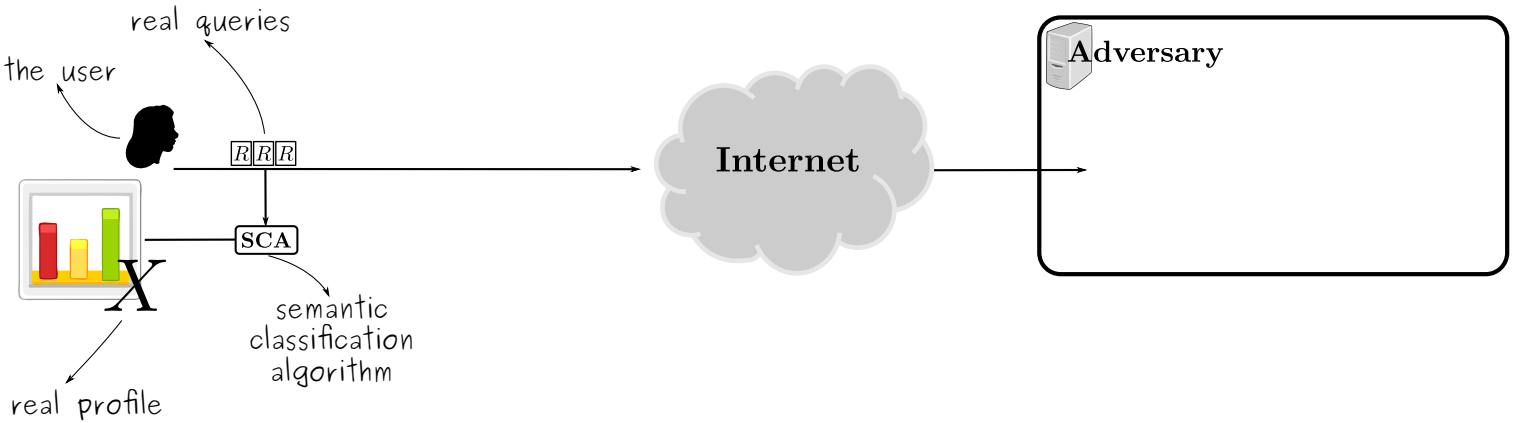
Our contribution

- General model.
- Evaluation framework
  $\Rightarrow$ with relevant privacy properties (details in the paper).
- Analysis of 6 existing systems (4 in this talk).

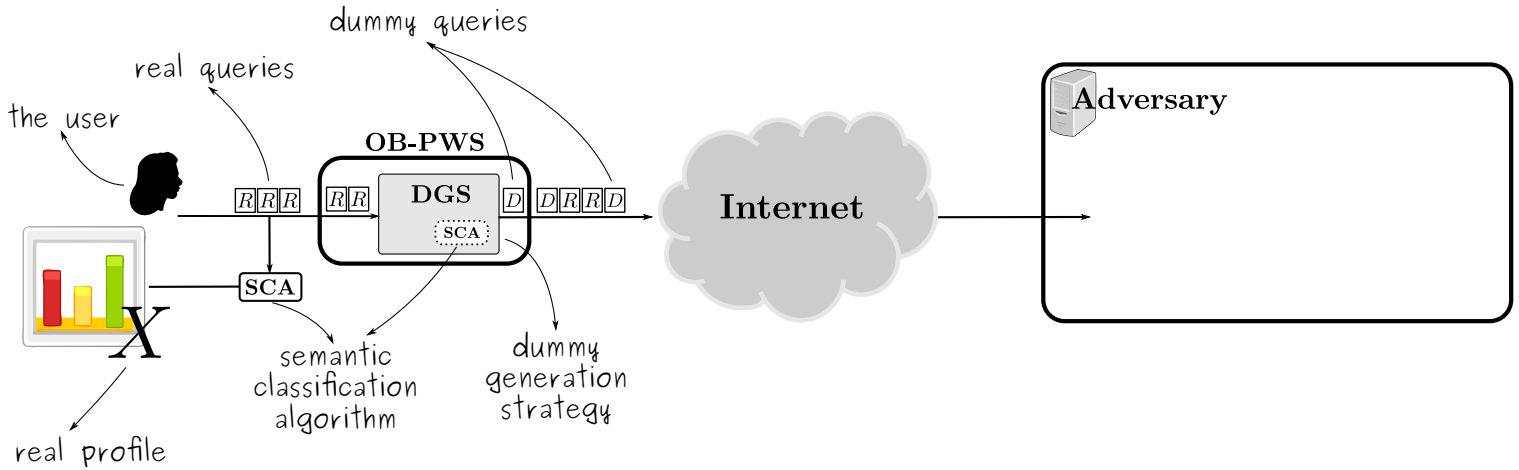
An abstract model for OB-PWS



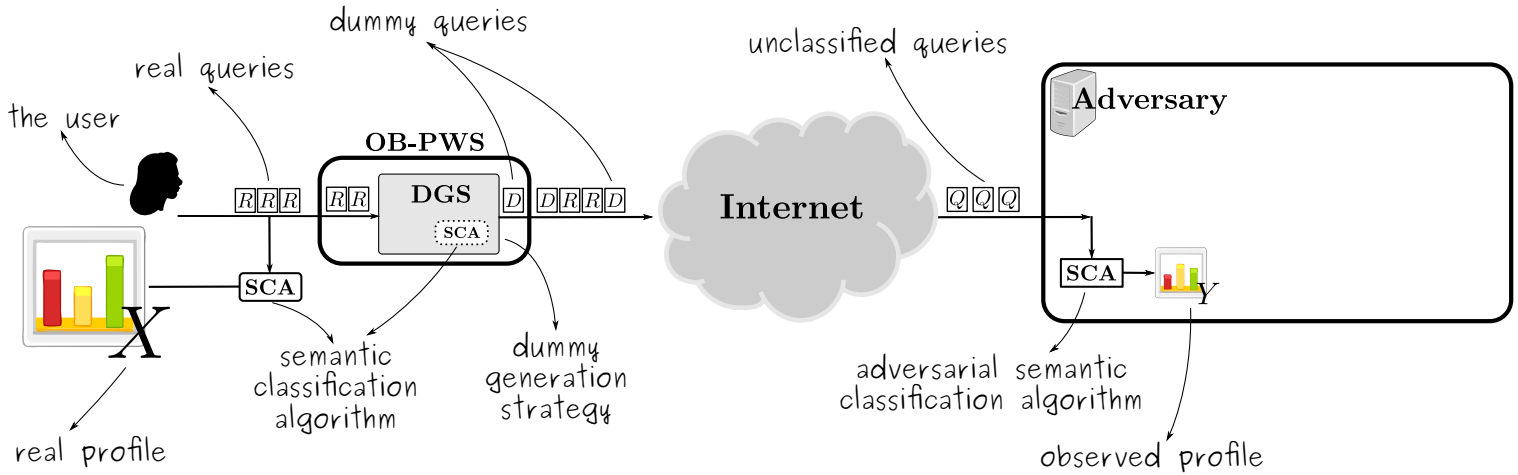
An abstract model for OB-PWS



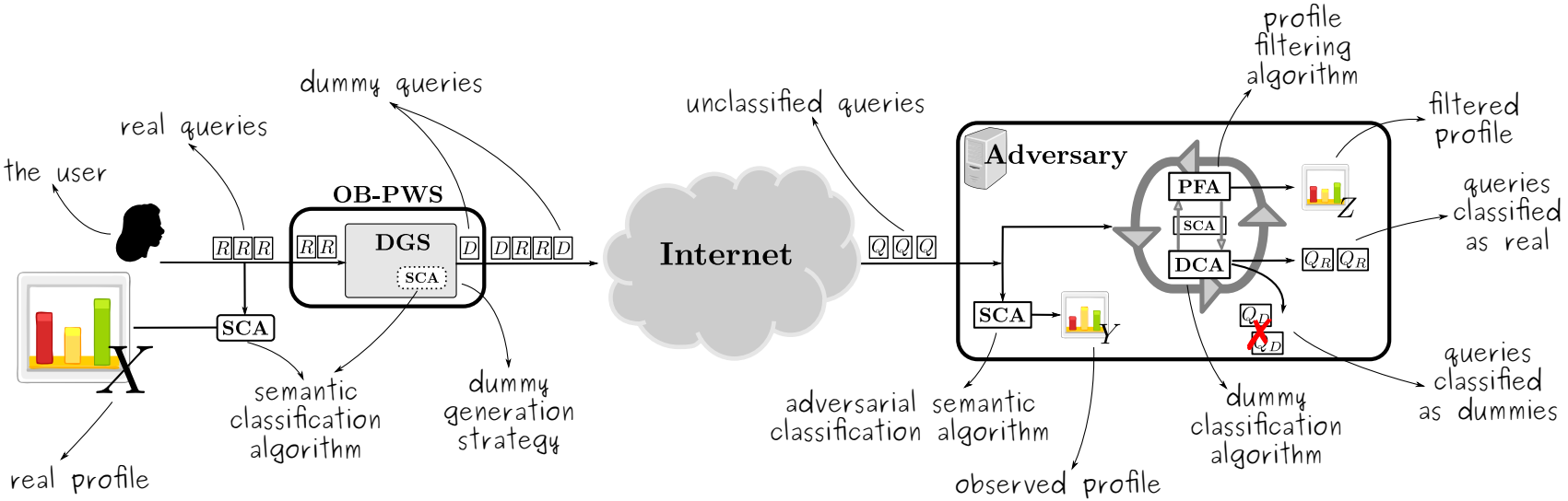
An abstract model for OB-PWS



An abstract model for OB-PWS



An abstract model for OB-PWS



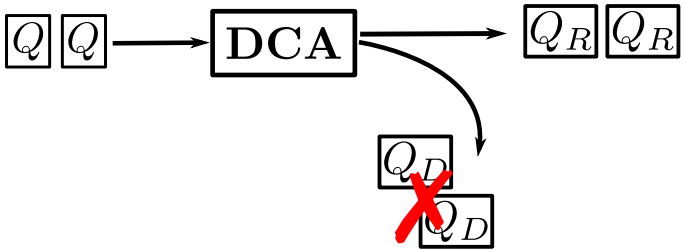
An Evaluation framework for DGS

A dual analysis is required:

An Evaluation framework for DGS

A dual analysis is required:

Query-Based Analysis

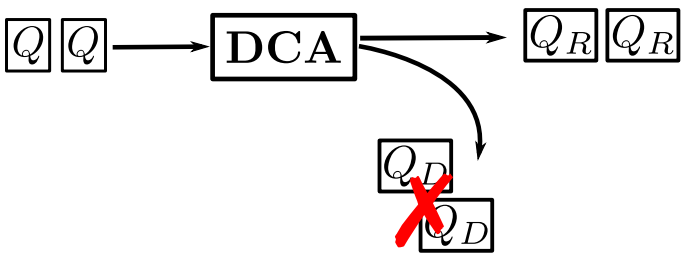


- Exploit vulnerabilities in the DGS to distinguish real from dummy queries.

An Evaluation framework for DGS

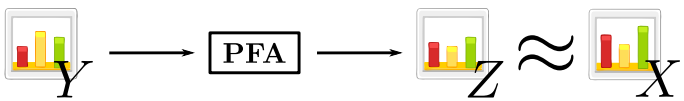
A dual analysis is required:

Query-Based Analysis



- Exploit vulnerabilities in the DGS to distinguish real from dummy queries.

Profile-Based Analysis

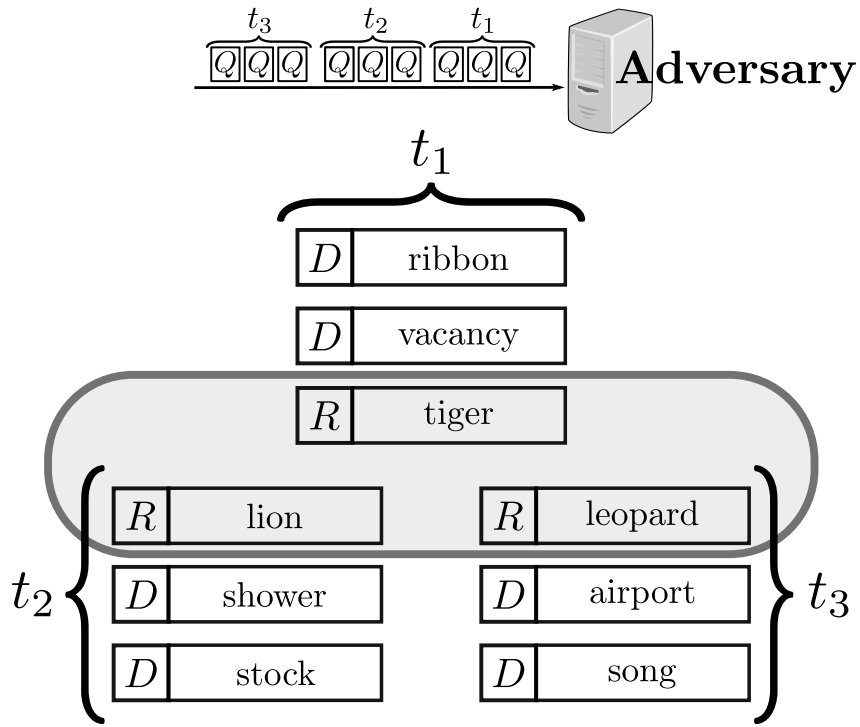


- Exploit vulnerabilities in the DGS to filter observed profile and recover the real profile.

GooPIR $h(k)$-Private Information Retrieval from Privacy-Uncooperative Queryable Databases [1]

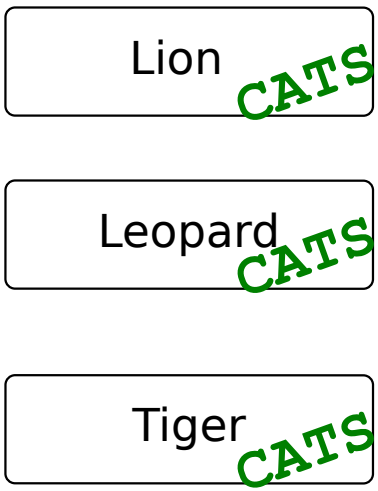
.

- A k-anonymity inspired approach.
- Prevents attacks based on:
  - Timing/metadata.
  - Popularity of queries.
  - Statistical disclosure.
- However does not consider the *topic* of the queries.

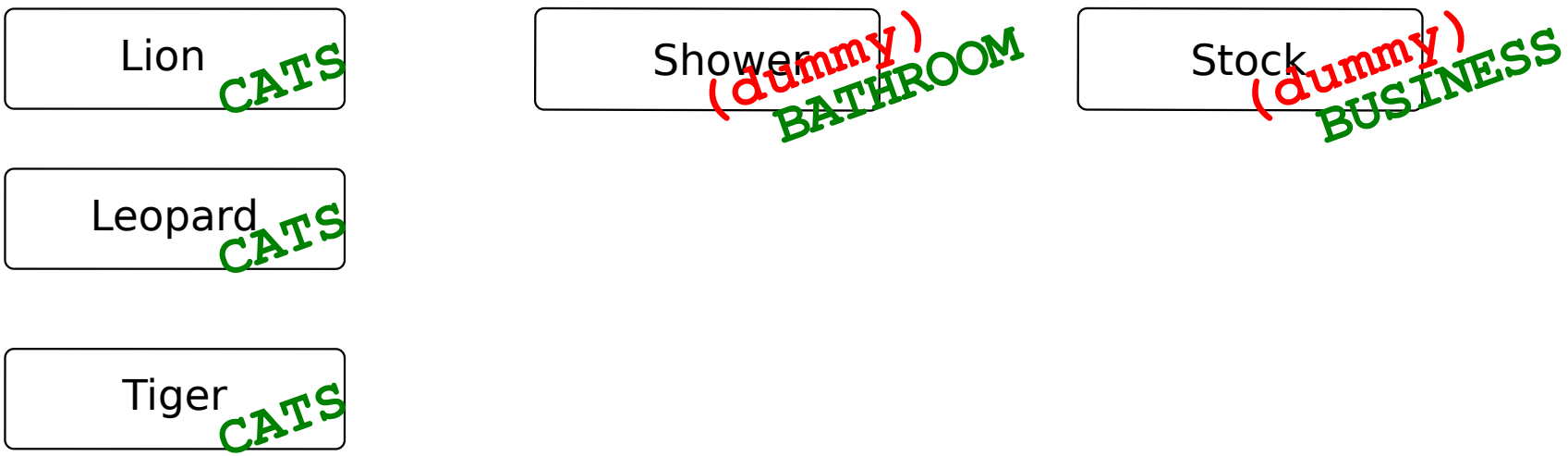


$\Rightarrow$ No dummy indistinguishability.

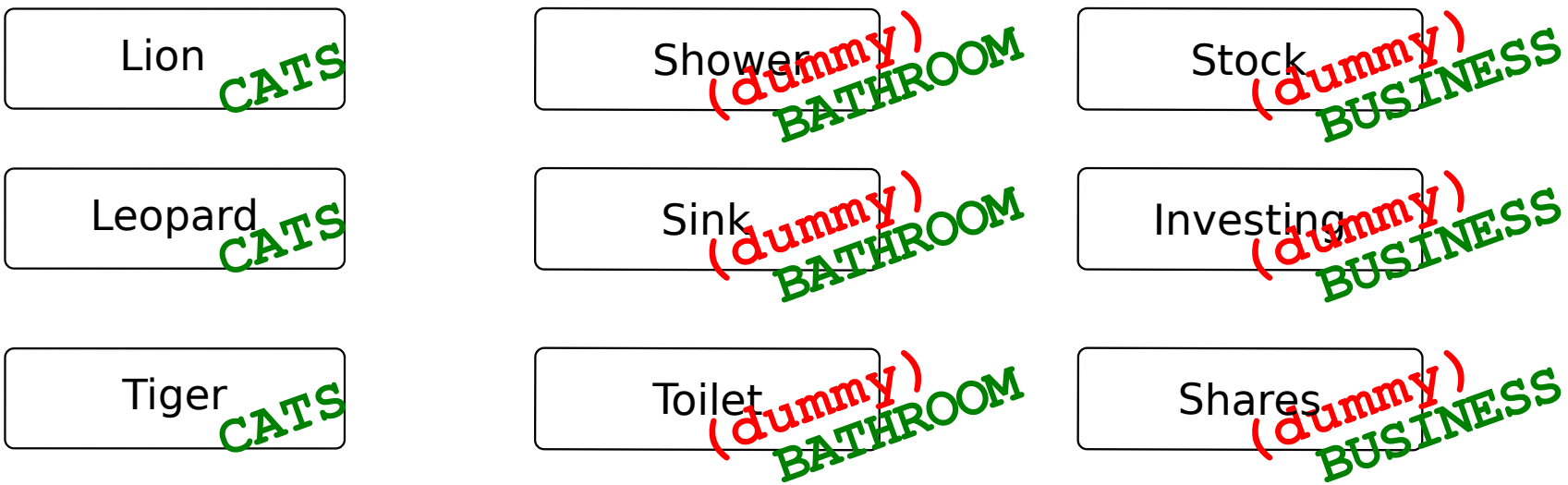
PDS Plausibly Deniable Search [2]



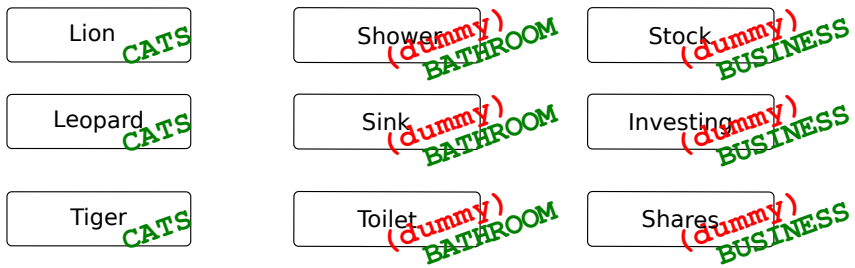
PDS Plausibly Deniable Search [2]

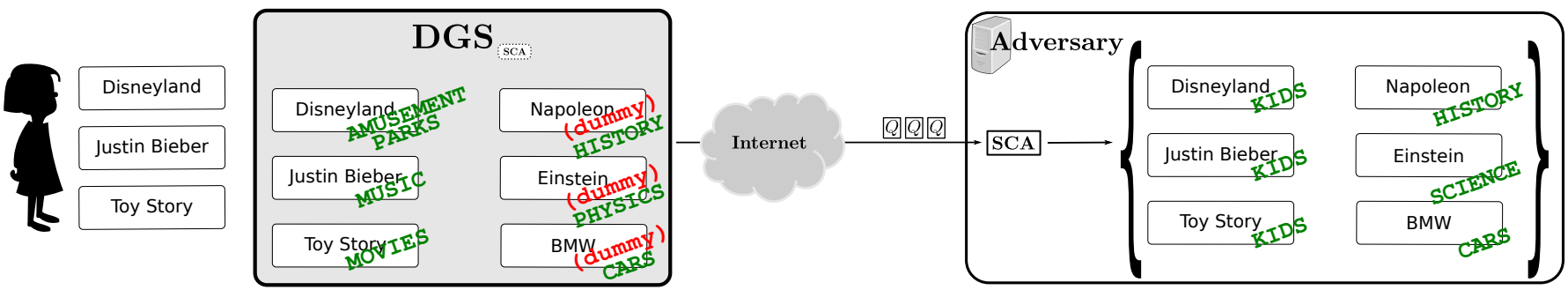


PDS Plausibly Deniable Search [2]



PDS Plausibly Deniable Search [2]



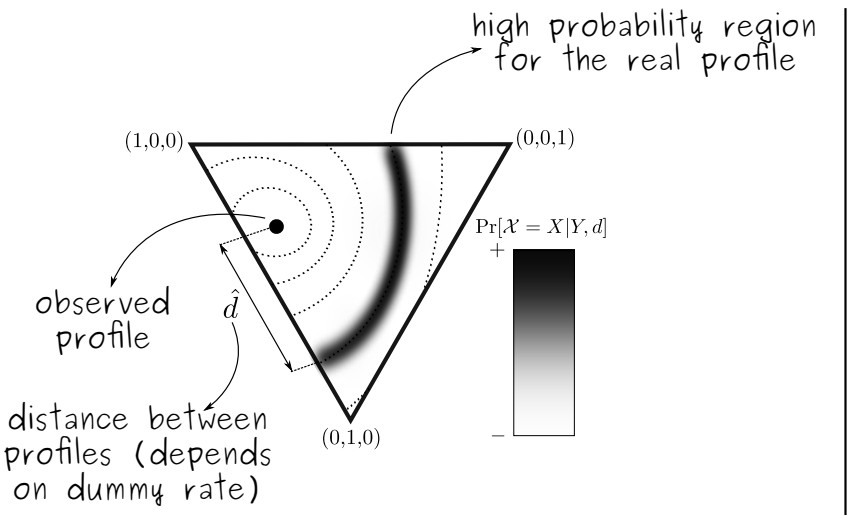


PRAW (A PRivAcy model for the Web) [3]

- Privacy = Dissimilarity.
- Dissimilarity $\propto$ amount of dummy queries.

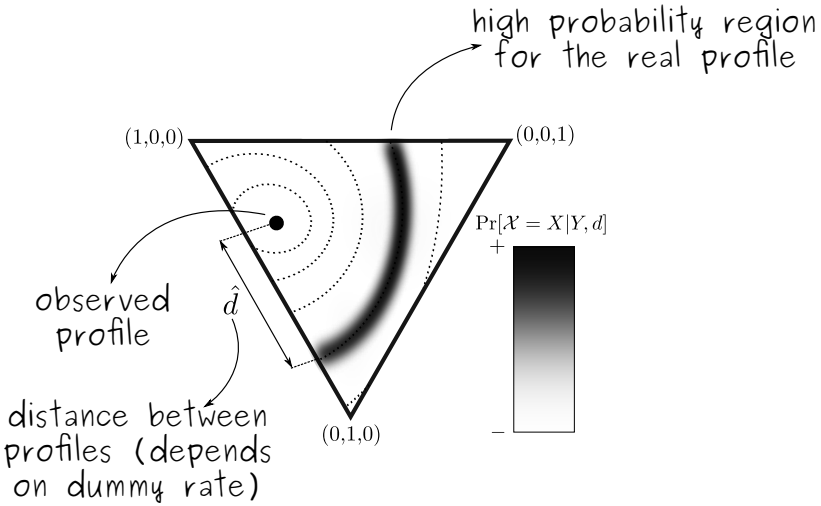
PRAW (A PRivAcy model for the Web) [3]

- Privacy = Dissimilarity.
- Dissimilarity $\propto$ amount of dummy queries.

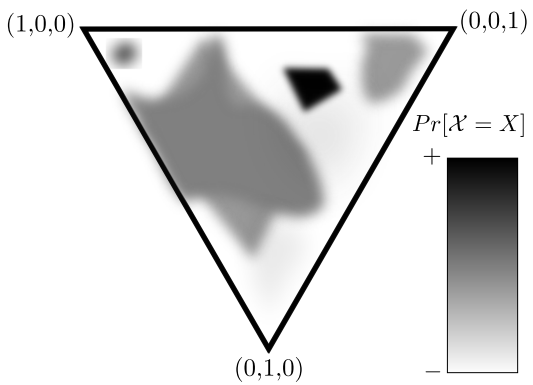


PRAW (A PRivAcy model for the Web) [3]

- Privacy = Dissimilarity.
- Dissimilarity $\propto$ amount of dummy queries.

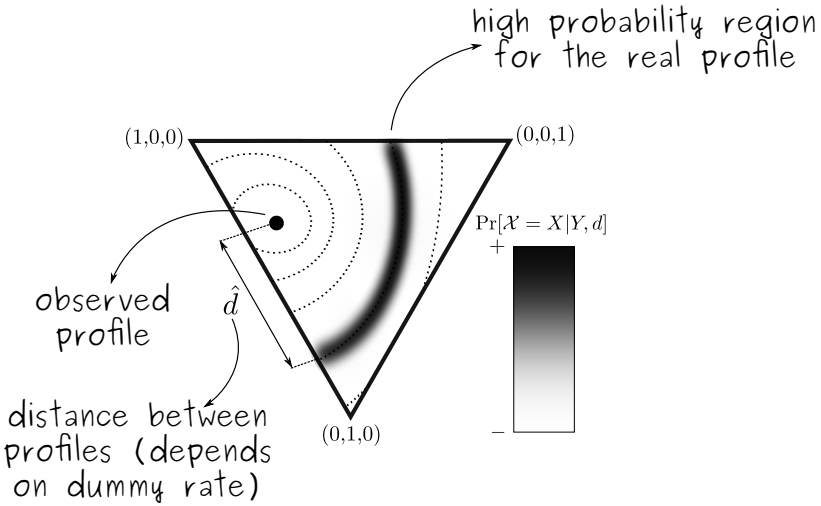


Considering prior information $\Pr[\mathcal{X} = X]$:

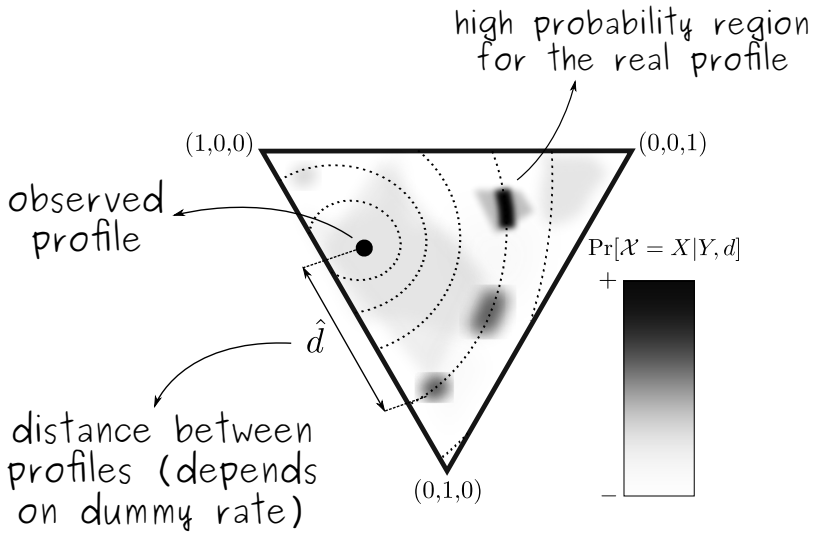


PRAW (A PRivAcy model for the Web) [3]

- Privacy = Dissimilarity.
- Dissimilarity $\propto$ amount of dummy queries.

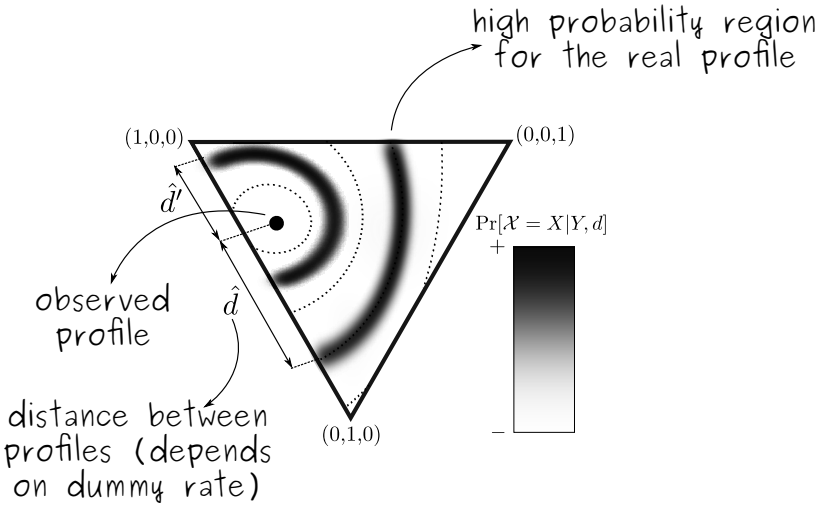


Considering prior information $\Pr[\mathcal{X} = X]$:

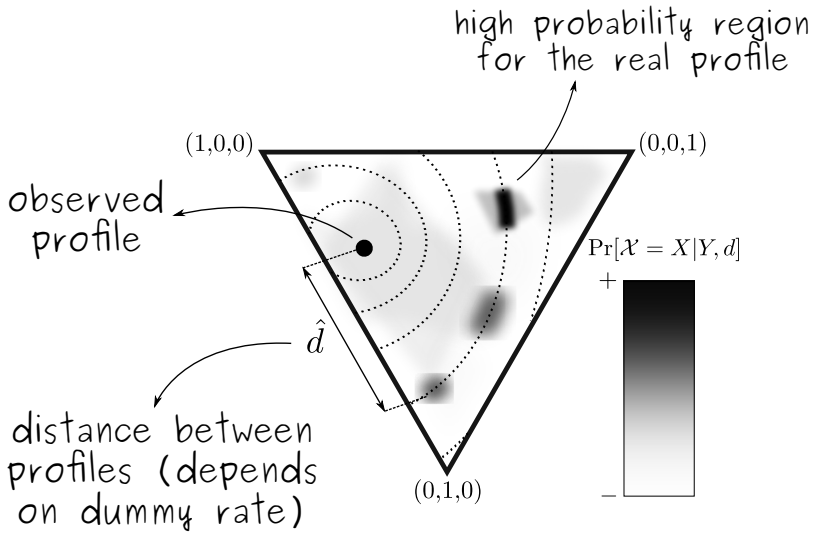


PRAW (A PRivAcy model for the Web) [3]

- Privacy = Dissimilarity.
- Dissimilarity $\propto$ amount of dummy queries.

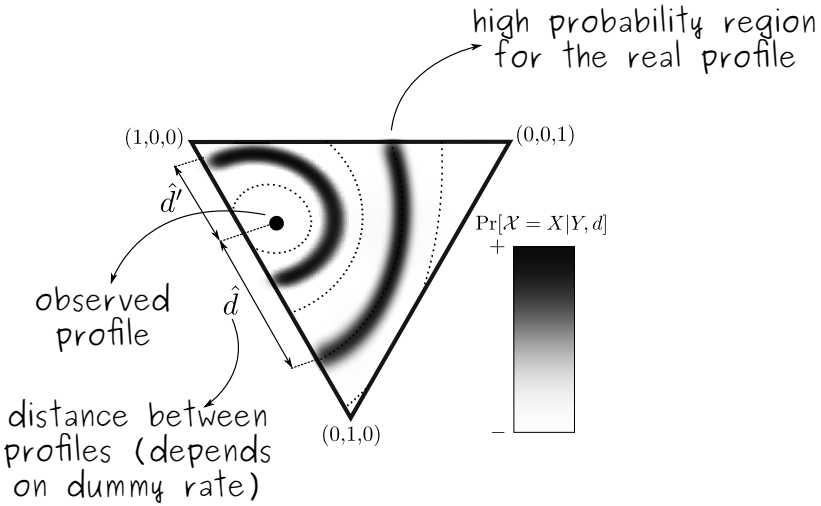


Considering prior information $\Pr[\mathcal{X} = X]$:

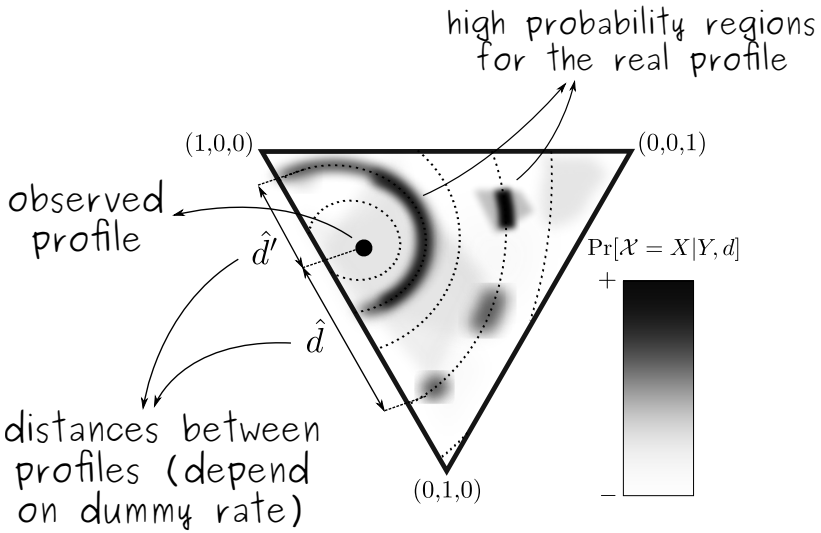


PRAW (A PRivAcy model for the Web) [3]

- Privacy = Dissimilarity.
- Dissimilarity $\propto$ amount of dummy queries.



Considering prior information $\Pr[\mathcal{X} = X]$:



OQF-PIR Optimized Query Forgery for Private Information Retrieval [4]

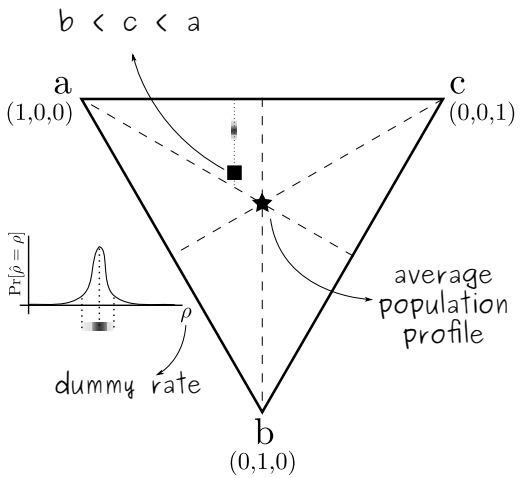
- Privacy = similarity to population's average profile.
- Exploitable features:
  - Known target profile.
  - Amount of dummy queries.
  - Waterfilling-based DGS.

OQF-PIR Optimized Query Forgery for Private Information Retrieval [4]

- Privacy = similarity to population's average profile.
- Exploitable features:
  - Known target profile.
  - Amount of dummy queries.
  - Waterfilling-based DGS.
- Query-based Analysis: Unpopular queries must be real.

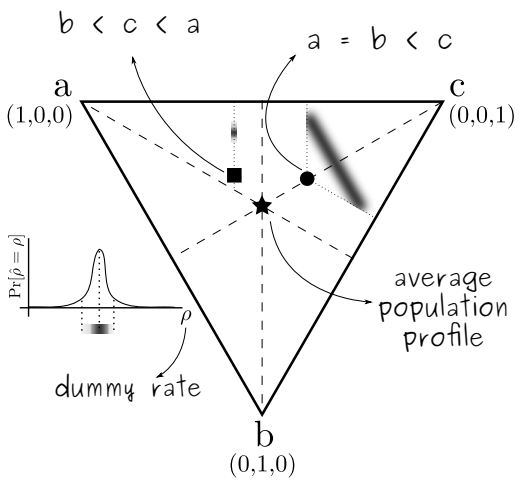
OQF-PIR Optimized Query Forgery for Private Information Retrieval [4]

- Privacy = similarity to population's average profile.
- Exploitable features:
  - Known target profile.
  - Amount of dummy queries.
  - Waterfilling-based DGS.
- Query-based Analysis: Unpopular queries must be real.
- Profile-based Analysis:



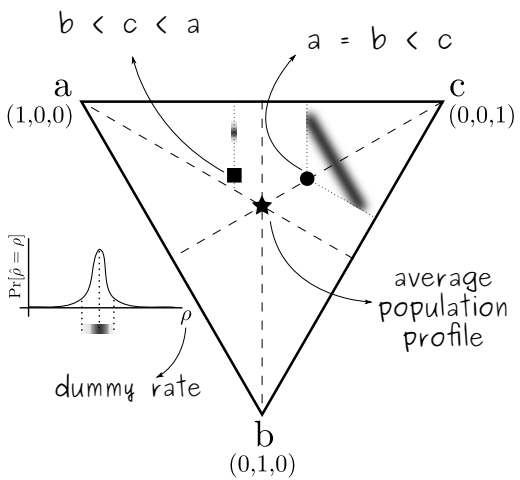
OQF-PIR Optimized Query Forgery for Private Information Retrieval [4]

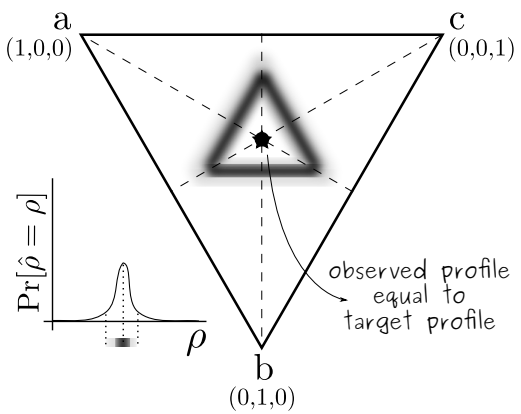
- Privacy = similarity to population's average profile.
- Exploitable features:
  - Known target profile.
  - Amount of dummy queries.
  - Waterfilling-based DGS.
- Query-based Analysis: Unpopular queries must be real.
- Profile-based Analysis:



OQF-PIR Optimized Query Forgery for Private Information Retrieval [4]

- Privacy = similarity to population's average profile.
- Exploitable features:
  - Known target profile.
  - Amount of dummy queries.
  - Waterfilling-based DGS.
- Query-based Analysis: Unpopular queries must be real.
- Profile-based Analysis:





Systems' Analysis Summary

- Two main categories of DGS:
  - Query based.
  - Profile based.
- Different definitions of what privacy means:
  - k-deniability.
  - The (dis)similarity of profiles.
- Ad-hoc analyses and evaluations.

Open problems and future work

- Plausibility of dummy queries, e.g., The dictionary issue.
- Adversarial modelling, e.g., Adversarial SCA issue.

Conclusions

- Abstract model for OB-PWS systems.
- Analysis framework
  $\Rightarrow$ Definition and formalization of relevant privacy properties.
- Analysis of 6 existing OB-PWS systems (4 in this talk).
- Both profile and query based analyses are needed!

Thank you.

Questions?

Main references:

[1] Josep Domingo-Ferrer, Agusti Solanas, and Jordi Castellà-Roca.
h(k)-private information retrieval from privacy-uncooperative queryable databases.
Online Information Review, 33(4):720–744, 2009.

[2] Mummoorthy Murugesan and Christopher W. Clifton.
Plausibly Deniable Search.
In *Proceedings of the Workshop on Secure Knowledge Management (SKM 2008)*, November 2008.

[3] Bracha Shapira, Yuval Elovici, Adlay Meshiach, and Tsvi Kuflik.
PRAW - A PRivAcy model for the Web.
JASIST, 56(2):159–172, 2005.

[4] David Rebollo-Monedero and Jordi Forné.
Optimized query forgery for private information retrieval.
IEEE Transactions on Information Theory, 56(9):4631–4642, 2010.