USENIX Security '24

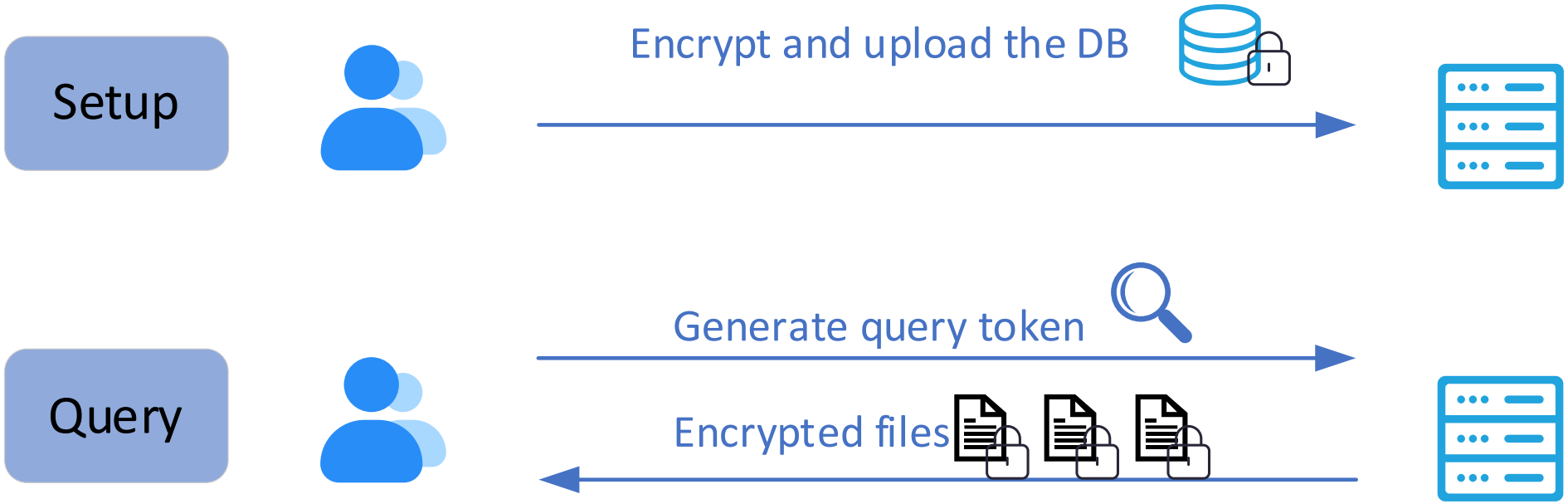
Query Recovery from Easy to Hard: Jigsaw Attack against SSE

Hao Nie, Wei Wang, Peng Xu, Xianglong Zhang, Laurence T. Yang, and Kaitai Liang*

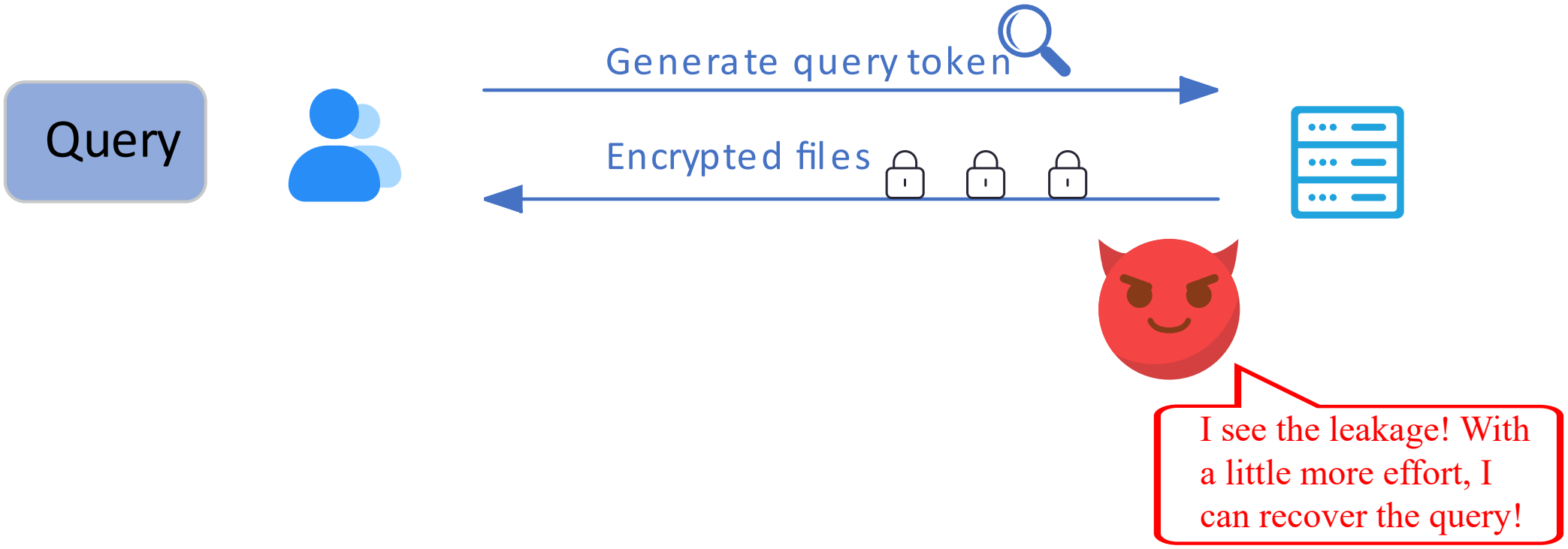
Huazhong University of Science and Technology
**Delft University of Technology*

Ⅰ. Motivations

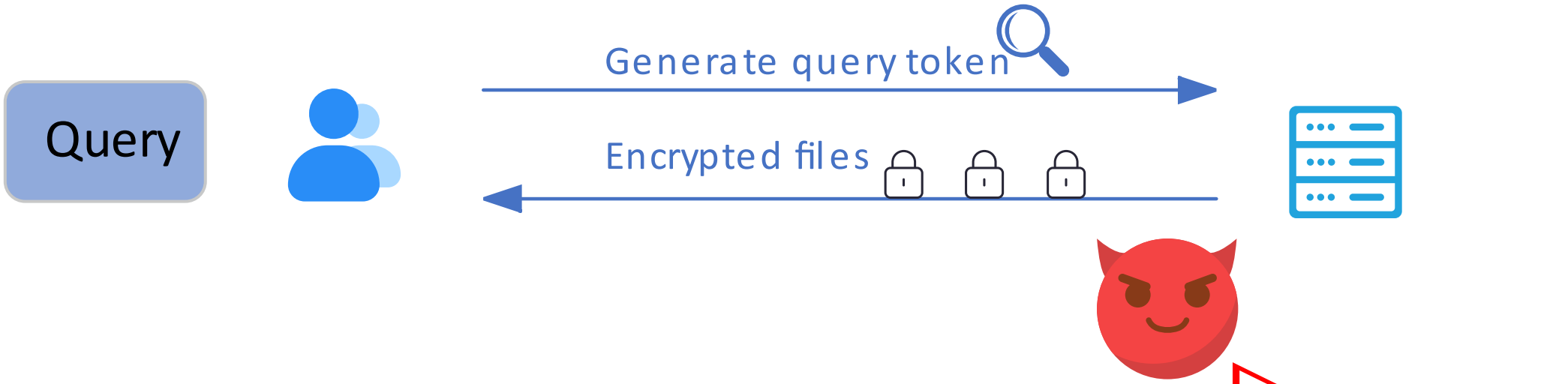
Searchable Symmetric Encryption



Searchable Symmetric Encryption

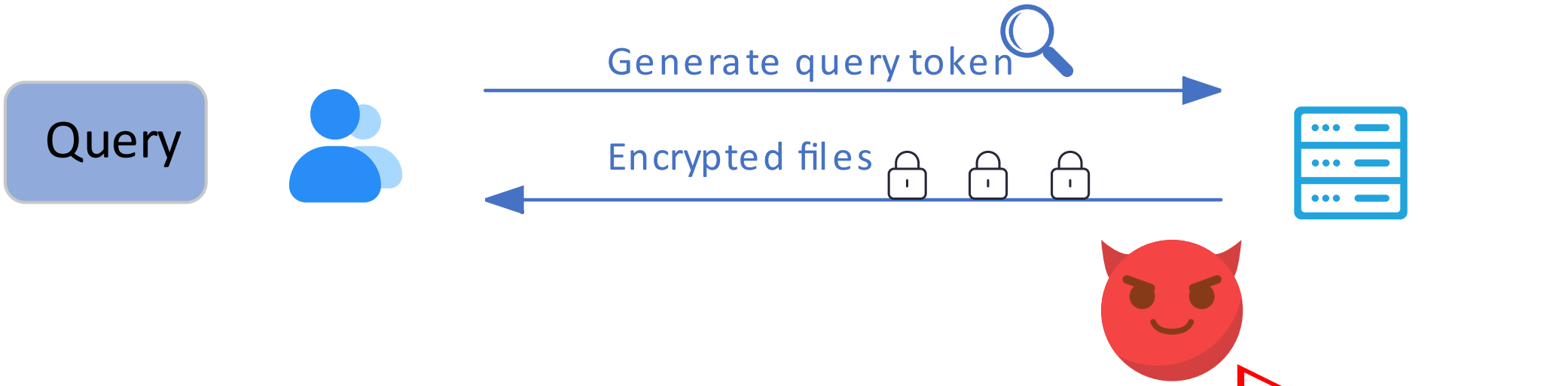


Searchable Symmetric Encryption



- The leakage often used in attacks includes:
  - Access Pattern, which reveals the identities of matched documents.
  - Volume Pattern, which reveal the number of matched documents.
  - Search Pattern, which indicates whether two queries are identical.

Searchable Symmetric Encryption



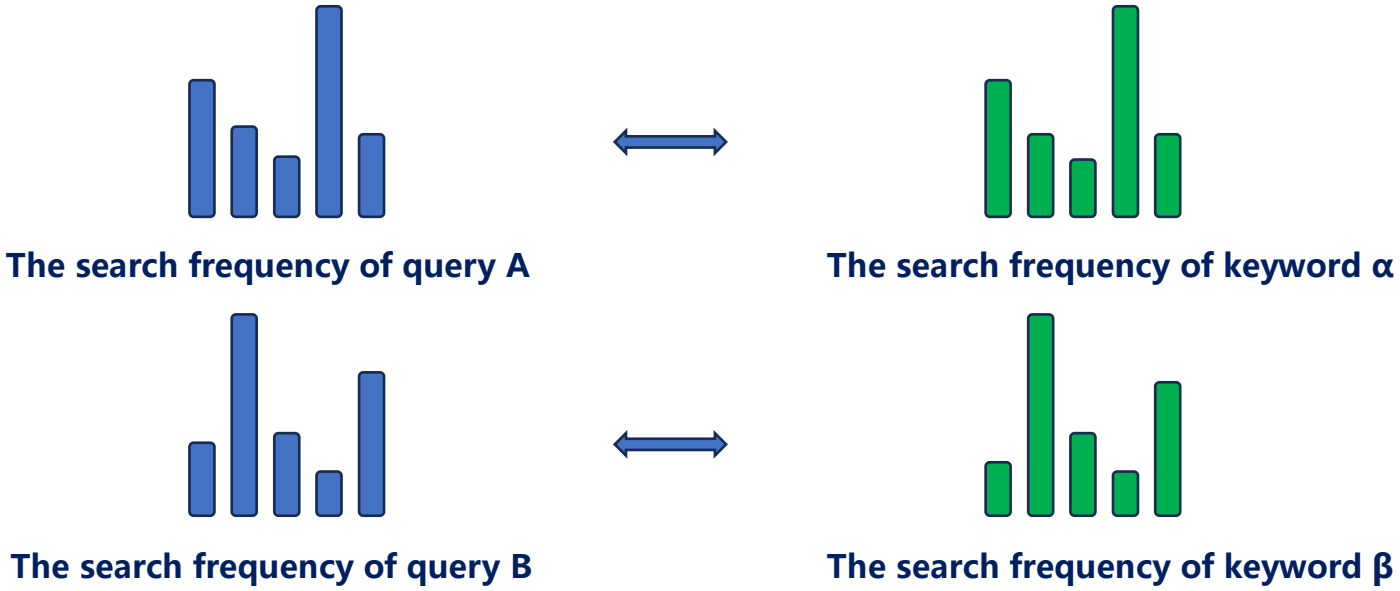
Client's data:

Known-data Attacker has partial client's data:

Similar-data Attacker has data similar to client's:

Previous Similar-data Attacks

- Liu et al. [LZWT14] use the query frequency (from the search pattern) to match queries with keywords.

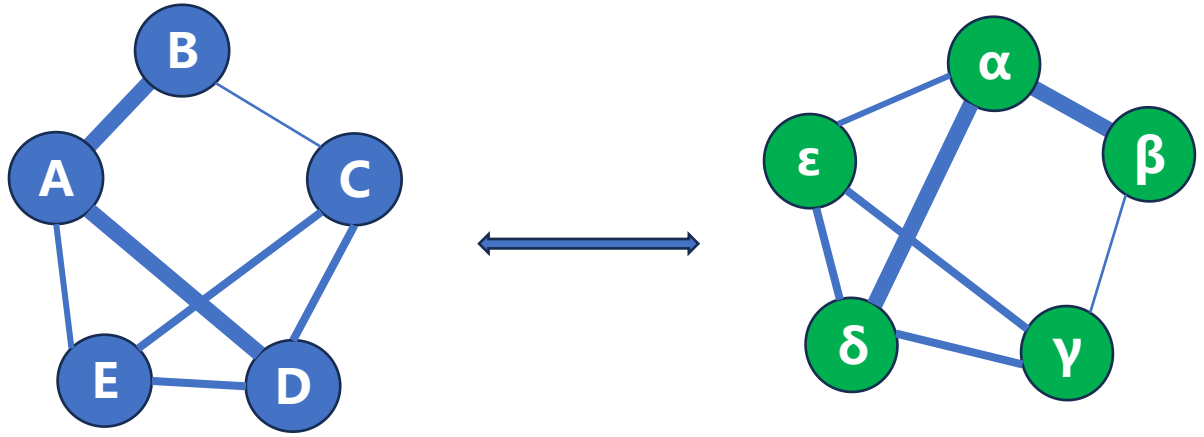


Query frequency observed from the leakage.

Keyword frequency from the prior knowledge.

Previous Similar-data Attacks

- Liu et al. [LZWT14] use the query frequency (from the search pattern) to match queries with keywords.
- Pouliot et al. [PW16], Damie et al. [DHP21], and Oya et al. [OK23] use the query co-occurrence to match queries with keywords.
  - The query co-occurrence is the probability of two queries shown in the same document. It could be deduced from the search pattern and access pattern.



Co-occurrence of queries from the leakage

Co-occurrence of keywords in the similar-data

Our Observations

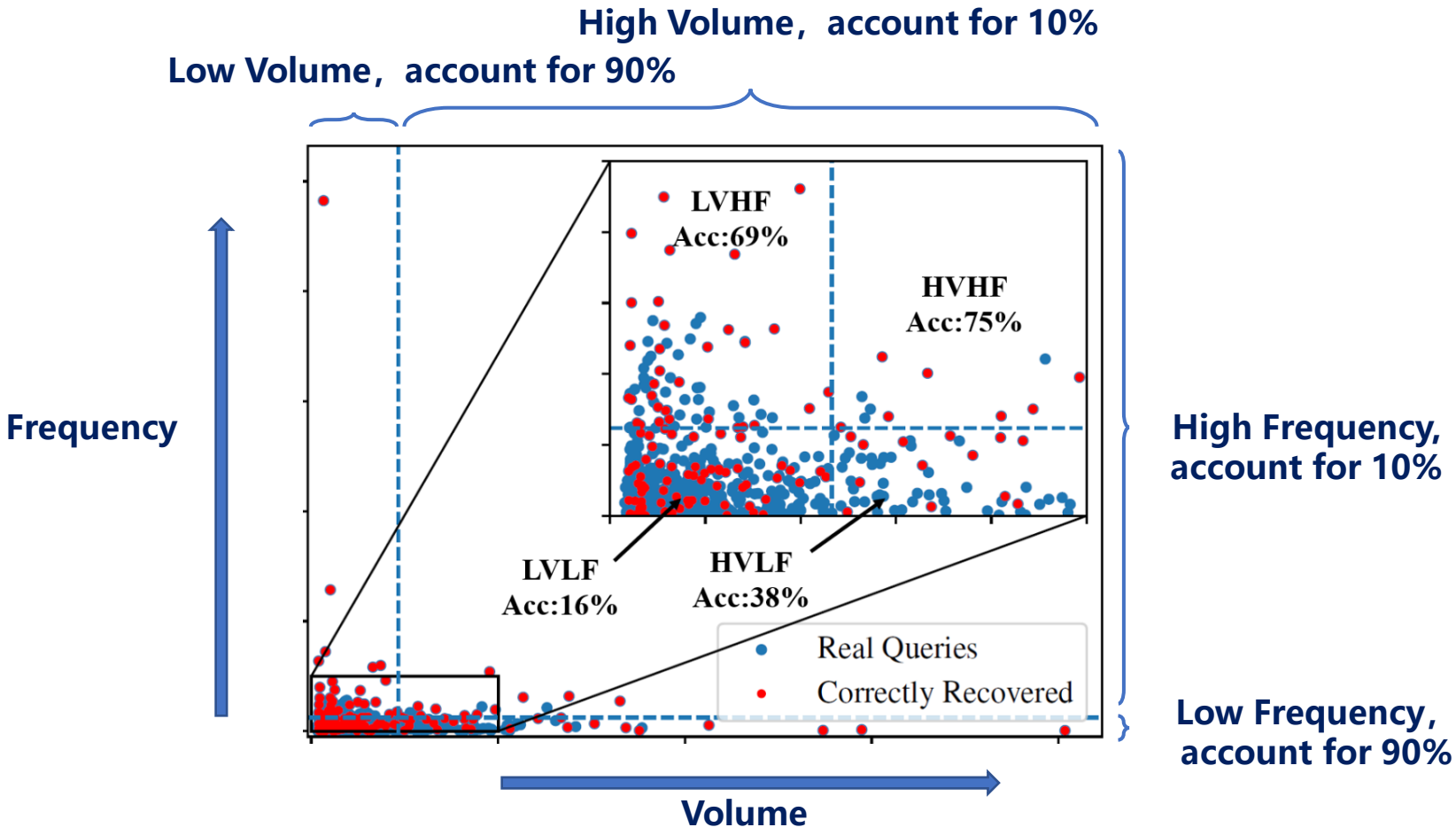
- 1. A small number of cracked queries can pose a significant threat to the security of other queries.
  - Damie et al. [DHP21] proposed the refined score attack that achieves around 85% accuracy in recovering all queries by utilizing only 10 known queries.

Our Observations

- 1. A small number of cracked queries can pose a significant threat to the security of other queries.
- 2. Queries with a high volume/frequency are much easier to recover than others.
  - In a database, the volume and frequency of keywords follows Zipf's law.
  - Queries with higher volume or frequency display larger disparities, which consequently makes it easier for attackers to recover those queries.

Our Observations

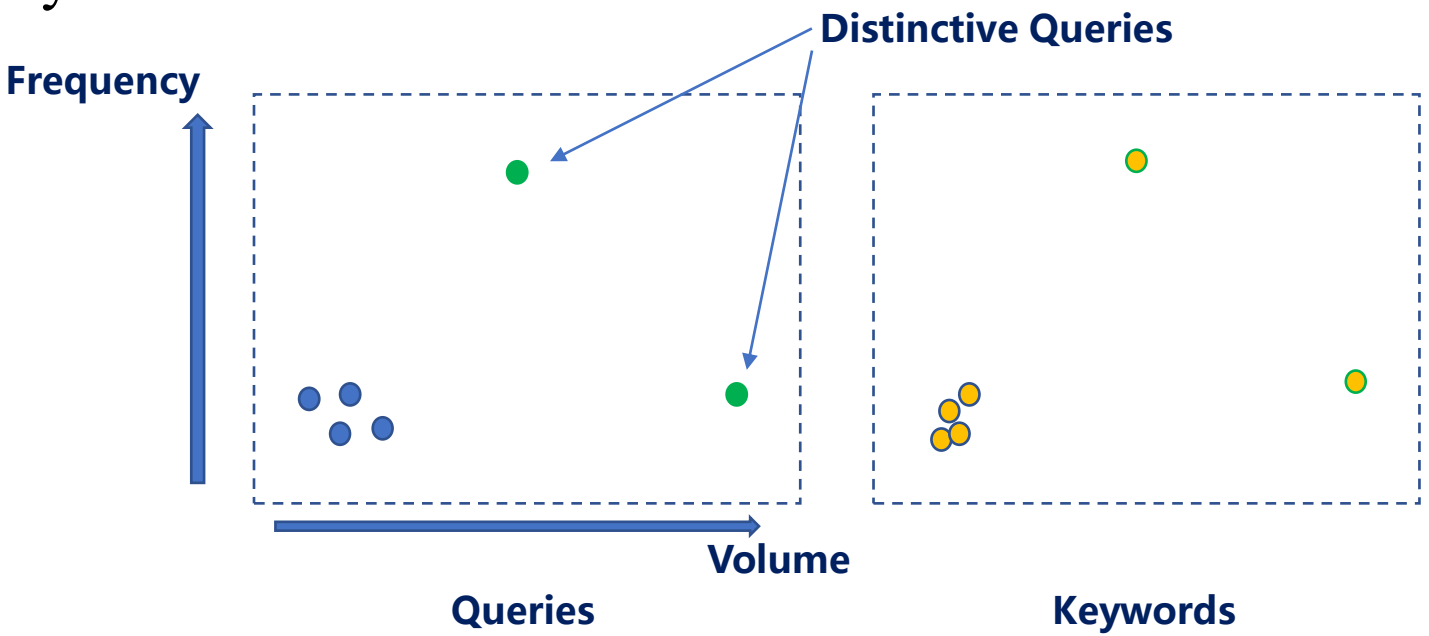
- A simple attack, which just matches the queries with keywords that have the closest volume and frequency, has 75% accuracy on the HVHF quadrant.



Ⅱ. Our attack

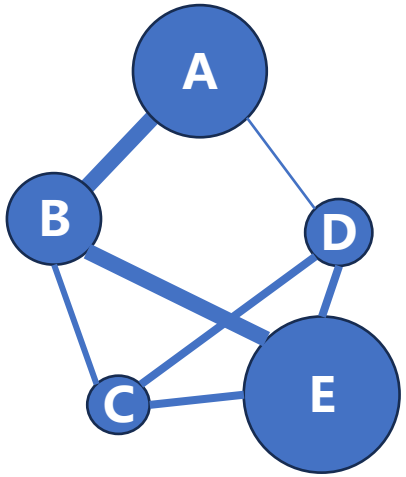
Jigsaw - Module 1

- Identify and recover the distinctive queries:
  - Calculate the distance between all queries and their nearest neighbors, and select the first BaseRec queries with biggest distance as the distinctive queries.
  - Match the BaseRec queries to the keywords that have the closest volume and frequency.

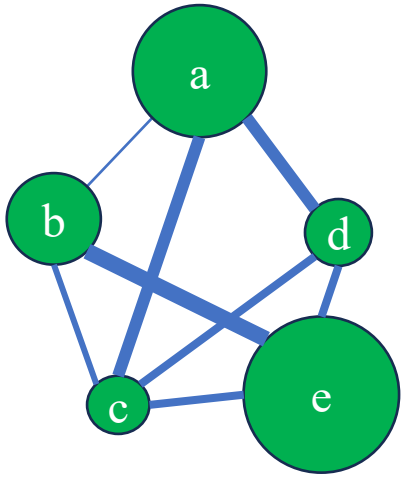


Jigsaw - Module 2

- Remove some ill-matched queries:
  - We check whether the results of module 1 is good or not. The good ones should also match in the co-occurrence relations. We keep ConfRec matched queries in this module.



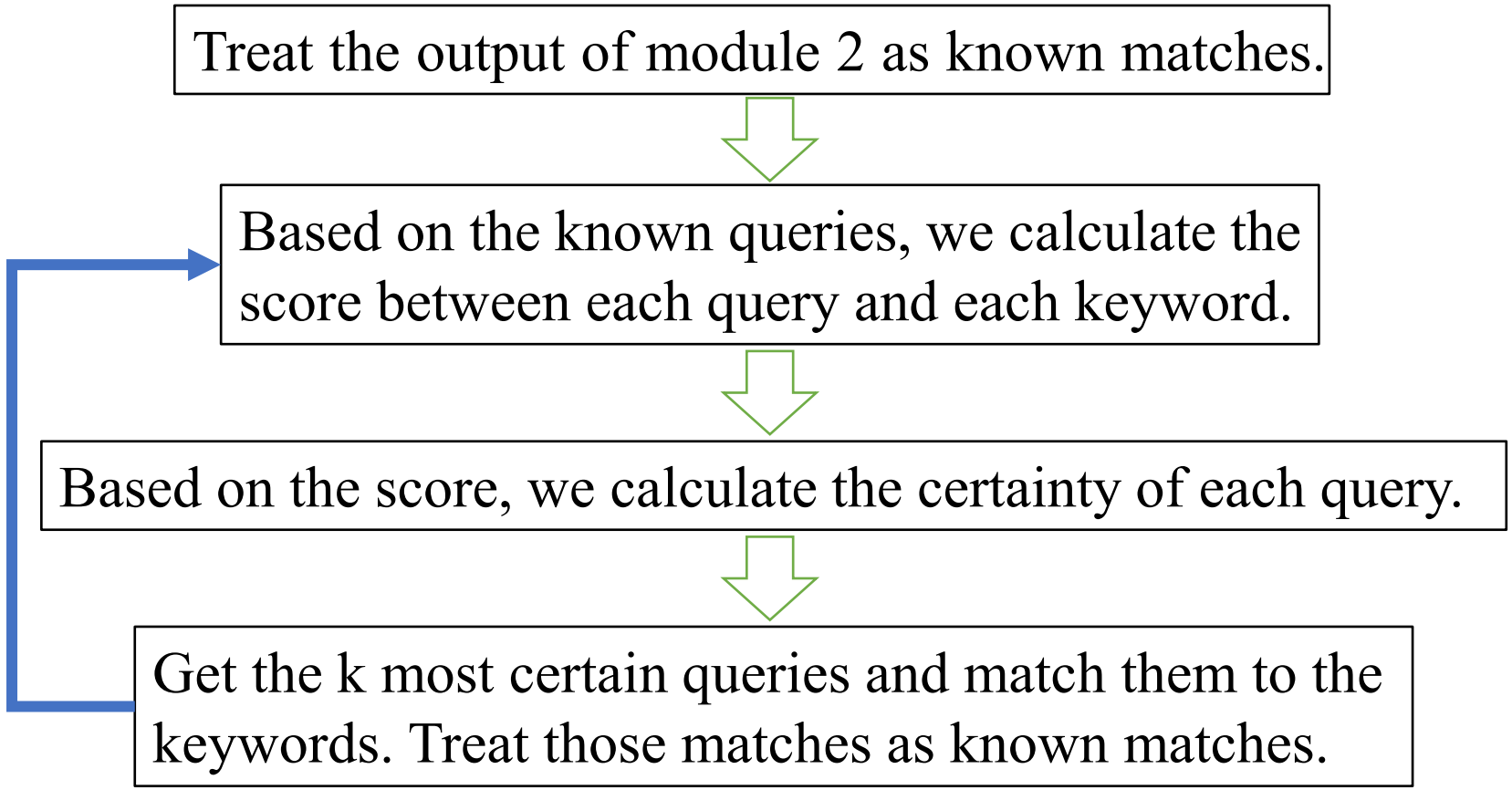
Recovered queries and their co-occurrence relations.



The corresponding keywords and their co-occurrence relations.

Jigsaw - Module 3

- Recover all queries based on the output of module 2:



Jigsaw – Experimental Results

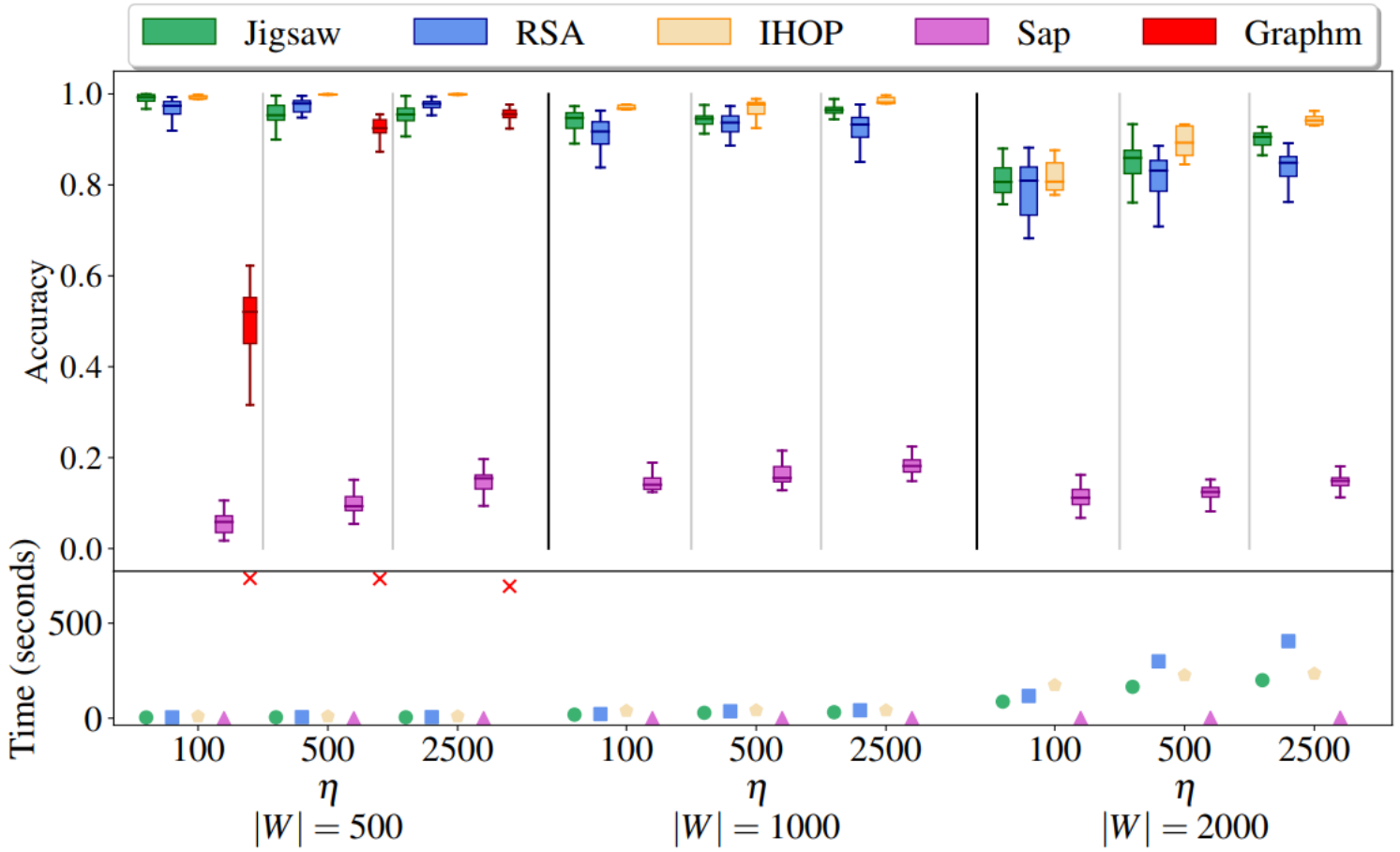


Figure: Jigsaw vs RSA[DHP21] vs IHOP[OK23] vs Sap[OK21] vs Graphm[PW16] in accuracy and runtime.

Jigsaw – Experimental Results

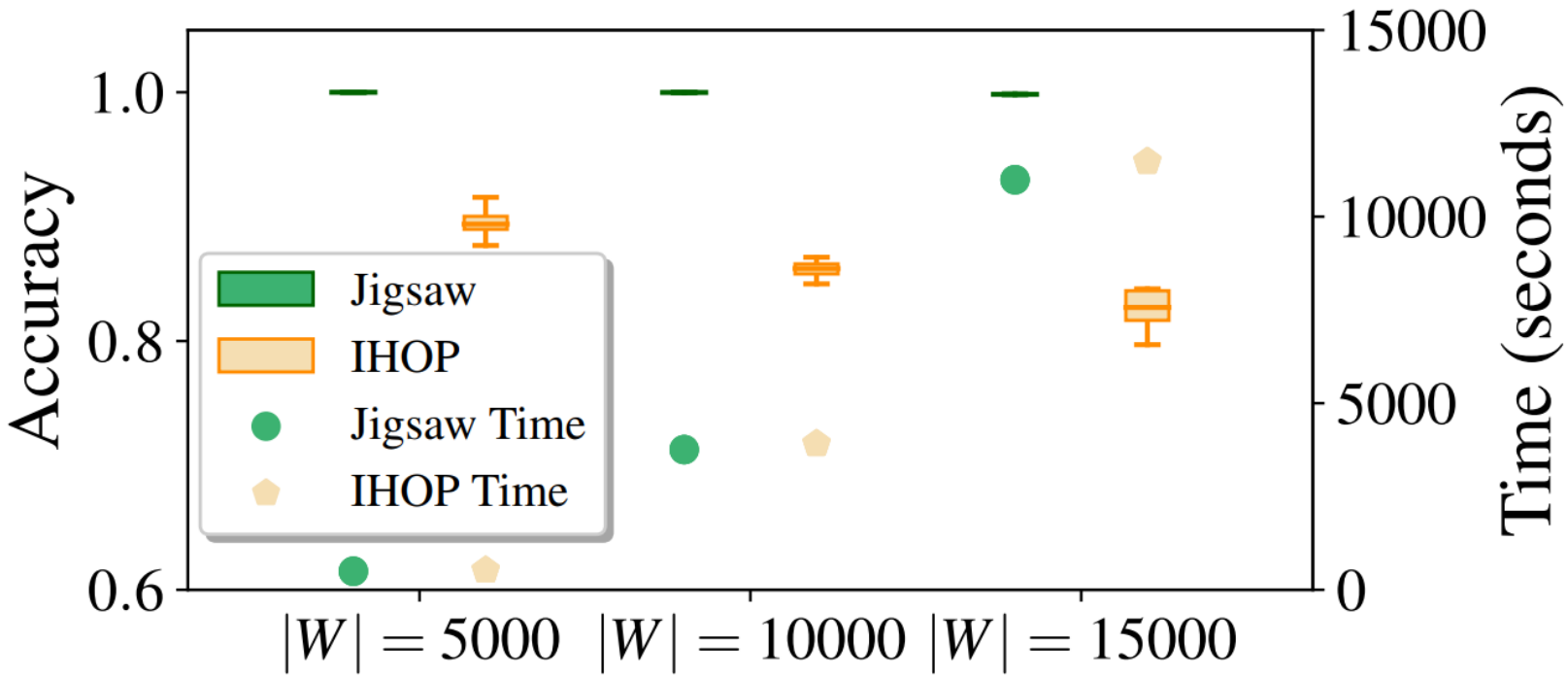
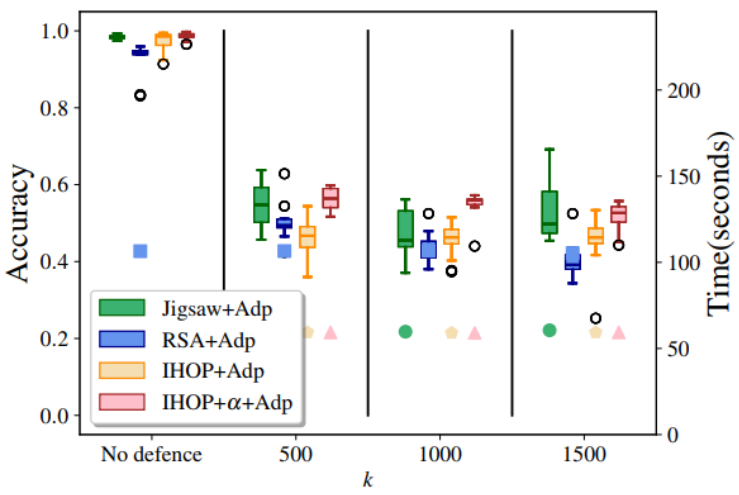
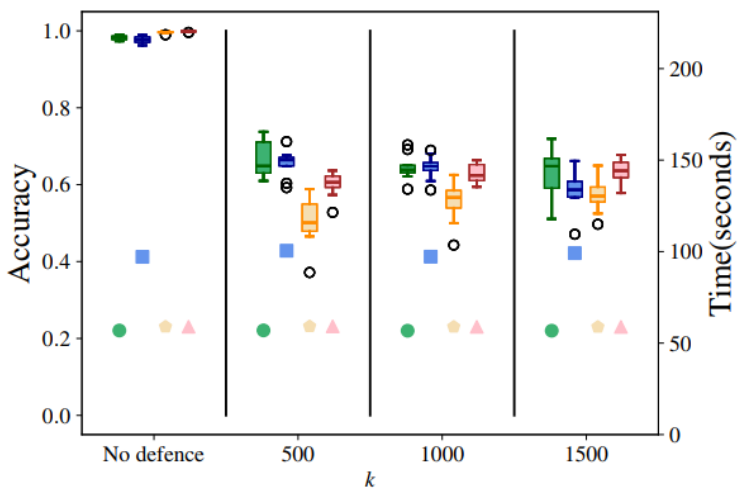


Figure: Jigsaw vs IHOP in accuracy with the same time limits.

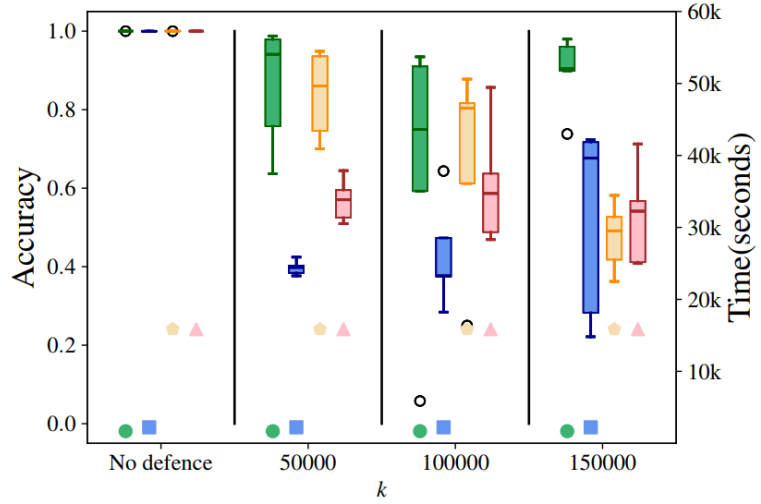
Against Countermeasures



Enron
(|W|=1000)



Lucene
(|W|=1000)

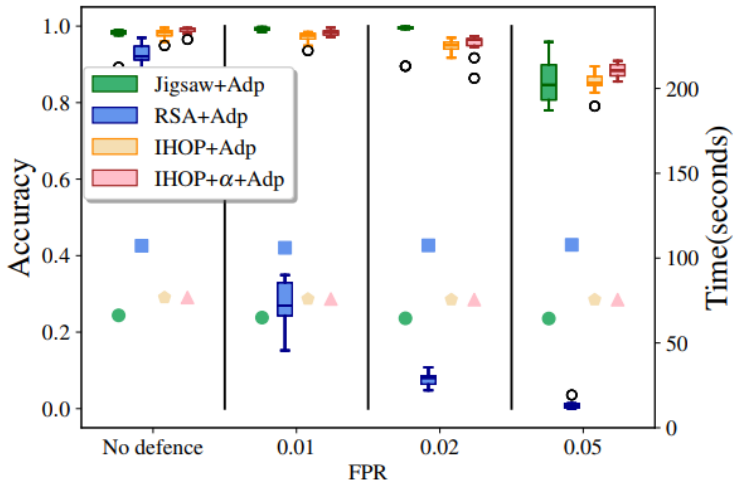


Wikipedia
(|W|=5000)

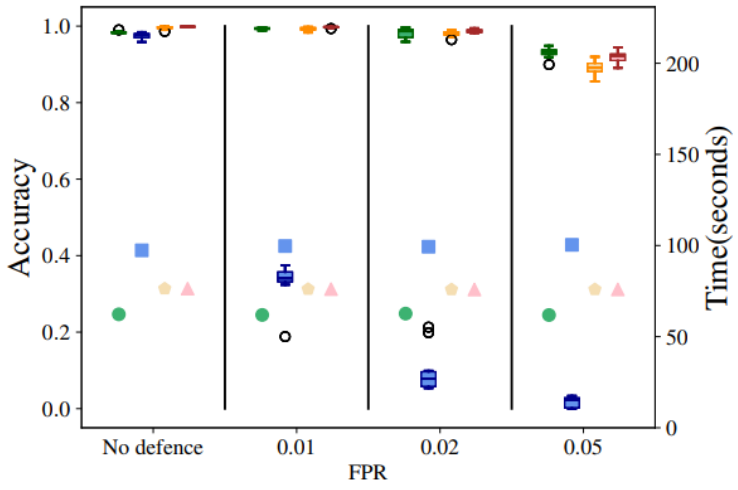
Figure: Jigsaw vs RSA vs IHOP in accuracy against the padding in [CGPR15].

- We pad the attacker's database with the same method as the client to minimizing the disparity between the similar data and the padded data.

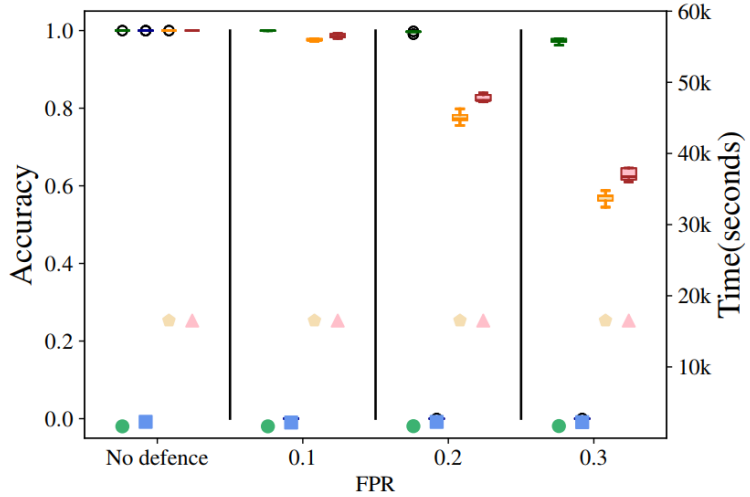
Against Countermeasures



Enron
(|W|=1000)



Lucene
(|W|=1000)



Wikipedia
(|W|=5000)

Figure: Jigsaw vs RSA vs IHOP in accuracy against the obfuscation in [CLRZ18].

- We use the similar adaptation as [OK23] to all the attacks.

Ⅲ. Conclusion

Conclusion

- We propose a new similar-data attack, Jigsaw. Some distinctive queries could threaten the whole system due to an attack like Jigsaw.

- Jigsaw could bypass some countermeasures and still has high accuracy due to that the countermeasures do not protect the distinctive queries well.

- An effective defense should hide the distinctive queries.

Thank you for listening!

Code available: https://github.com/JigsawAttack/JigsawAttack

Contact information:

→ niehao@hust.edu.cn

→ viviawangwei@hust.edu.cn

→ xupeng@hust.edu.cn