Peer2PIR: Private Queries for IPFS

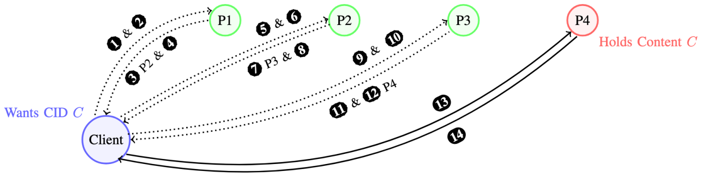
Miti Mazmudar, Shannon Veitch, Rasoul Akhavan Mahdavi

Introducing IPFS

- A peer-to-peer distributed file system [1]
- Backbone of distributed web applications
  - Fleek, Space Daemon, …
- Each Peer stores some of the content
- Content is accessible via Content Identifier (CID)
- Routing information is stored in Distributed Hash Table (DHT)
- Steps to retrieve a file:
  1. Peer Routing: What's the address of this Peer ID?
  2. Content Discovery: Which Peer holds content with this CID?
  3. Content Retrieval: Do you hold content with this CID?

The problem: All three steps reveal the user's desired content

		🔓 Standard IPFS	🔒 Ours (Peer2PIR)
····>	❶ ❺ ❾ Peer routing request	`Peers near Hash(C)?`	`PrivPeerRoutingQuery(C)`
	❷ ❻ ❿ Prov. advert. request	`Provs. for C?`	`PrivProvAdQuery(C)`
<····	❸ ❼ ⓫ Peer routing response	`PID`	`PrivPeerRoutingResp(PID)`
	❹ ❽ ⓬ Prov. advert. response	`PID/None`	`PrivProvAdResp(PID/None)`
⟶	⓭ Content retrieval request	`WantHave C? / WantBlock C`	`PrivWantHave(C)`
	⓮ Content retrieval response	`Have / Block C`	`PrivBlock(C)`



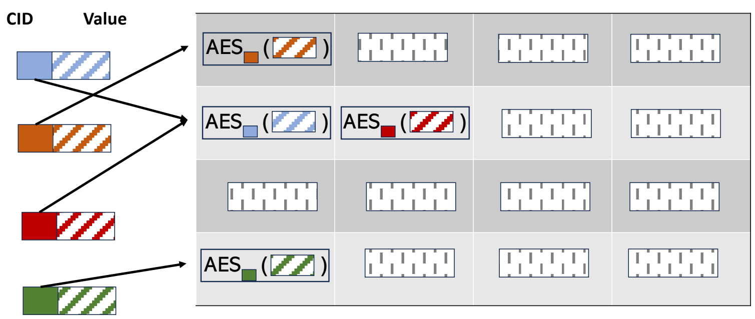
Our main tool: Private Information Retrieval (PIR)

Access database without revealing the query

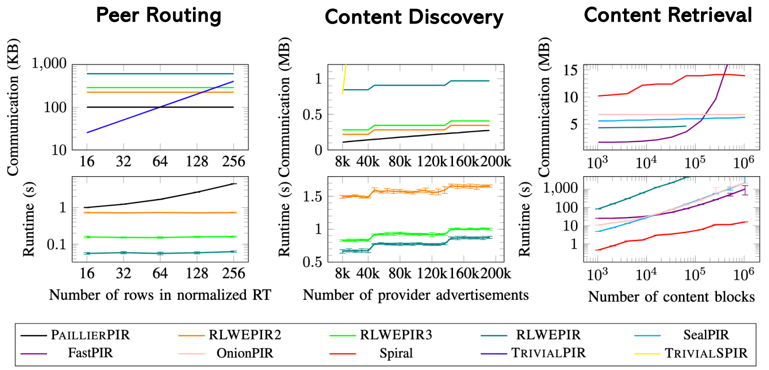
1. Routing Table
2. Provider Advertisements
3. Content store

1. Peer Identifier
2. Content ID
3. Content ID

Example: PIR for Private Content Discovery



Binned and Symmetrically Encrypted Database



[1] Trautwein et. al. 2022. Design and evaluation of IPFS: a storage layer for the decentralized web. In Proceedings of the ACM SIGCOMM 2022 Conference (SIGCOMM '22).

The Challenges

Assumptions of SOTA PIR protocols

- Amortized costs
- Tabular database
- Prior client-server connection
- Large databases

These assumptions don't hold in IPFS

Protocol	Key Material	Query (Encrypted)	Response (Plaintext)	Response (Encrypted)
SealPIR [5]	1.6 MB	90 KB	10 KB	181 KB
FastPIR [2]	0.67 MB	64 KB	10 KB	65 KB
OnionPIR [45]	5.4 MB	64 KB	30 KB	128 KB
Spiral [41]	13 MB	28 KB	7.5 KB	20 KB
HintlessPIR* [33]	-	453 KB	32 KB	3080 KB
YPIR* [42]	462 KB	384 KB	1 B	12 KB
PAILLIERPIR	1.14 KB	0.38 KB	0.38 KB	0.76 KB
RLWEPIR	750 KB	64 KB	7.5 KB	65 KB
RLWEPIR3	192 KB	64 KB	7.5 KB	65 KB
RLWEPIR2	128 KB	64 KB	7.5 KB	65 KB

Our PIR solutions: RLWEPIR, PaillierPIR

- No setup required
- Efficient for single queries
- Suitable for small databases
- Extendable to Symmetric PIR
- Extends to Keyword PIR using CIDs

Conclusion & Findings

- Private IPFS queries are possible with minimal change to the network
- PIR is a practical solution for privacy in IPFS queries
- Existing PIR protocols are not sufficient
- Custom-made PIR protocols for IPFS
- Future PIR protocols can be incorporated in our framework

Check out our paper & code!