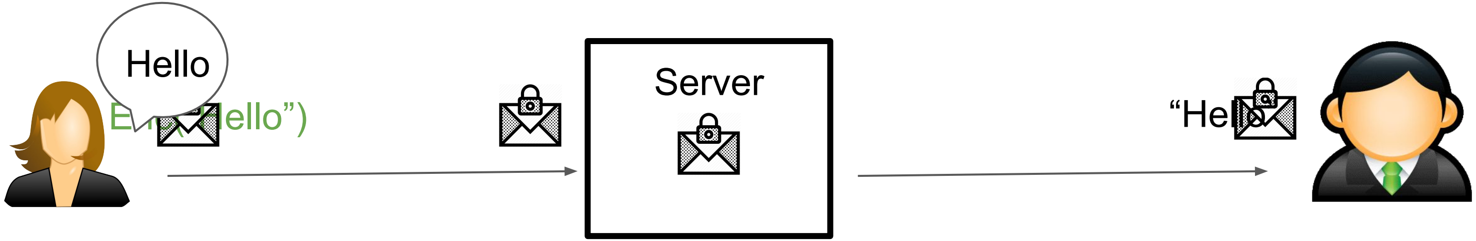
Addra: Metadata-private voice communication over fully untrusted infrastructure

Ishtiyaque Ahmad, Yuntian Yang, Divyakant Agrawal, Amr El Abbadi, and Trinabh Gupta

University of California, Santa Barbara

Voice calls are ubiquitous and contain sensitive content

Voice call providers enable end-to-end encryption



Content is hidden!

Not hidden:

- Participants
- Time
- Duration

Metadata

Does end-to-end encryption provide enough privacy?

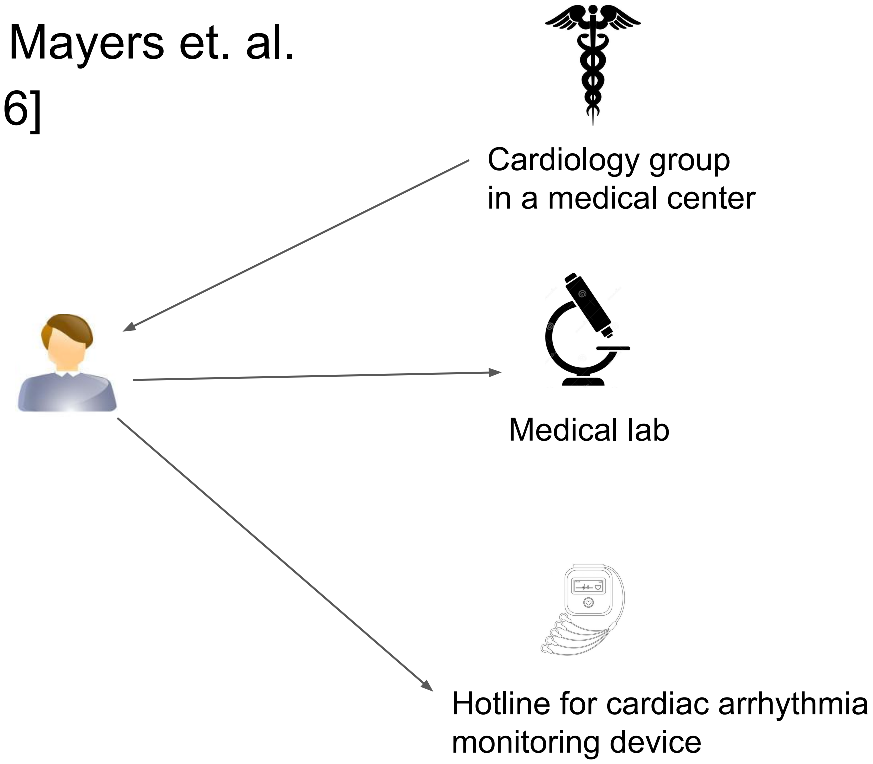
Metadata can be as revealing as content

> Metadata absolutely tells you everything about somebody's life.
>
> If you have enough metadata, you don't really need content.

Stewart Baker
Ex NSA General Counsel

Metadata can be as revealing as content

Study by Mayers et. al.
[PNAS ’16]



Cardiology group
in a medical center

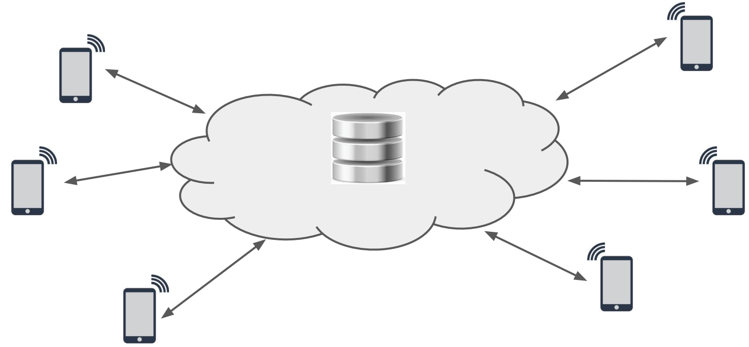
Medical lab

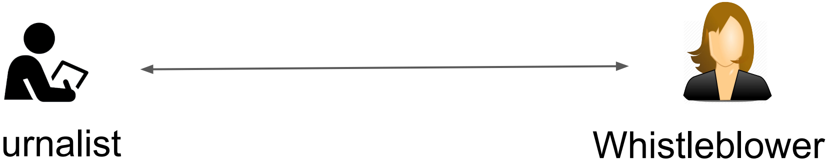
Hotline for cardiac arrhythmia
monitoring device

Cardiac
arrhythmia!

Metadata can be as revealing as content

Voice call metadata can be used for mass surveillance

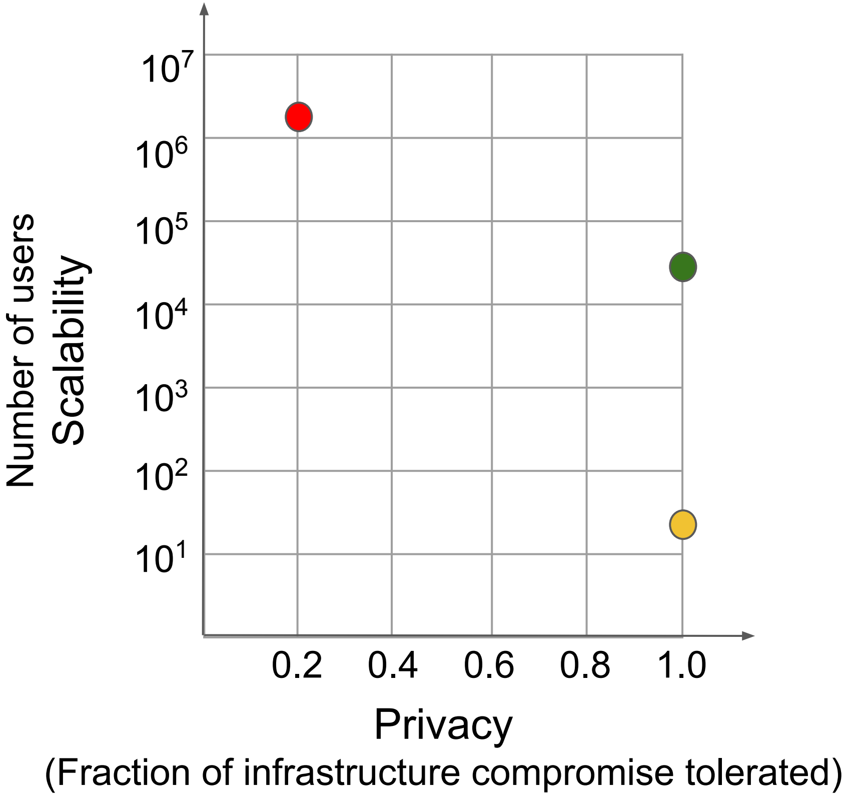




Deanonymized!

Can we make voice calls hiding metadata from a strong adversary?

Existing works either lack in scalability or privacy



🟡 DC-net based works

- Broadcasts messages

🔴 Yodel [SOSP ’19]

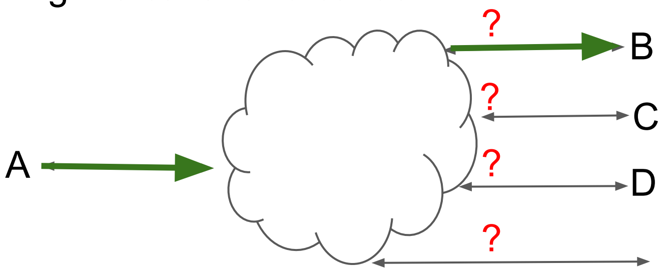
- Mixnet to shuffle messages

🟢 Addra

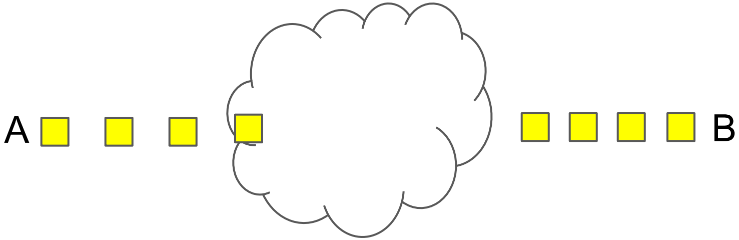
- No trust assumption
- Tolerates entire infrastructure compromise
- Scales to 32K users

Two key challenges

Challenge 1: Unlinking the caller and callee



Challenge 2: Scaling with low latency



Addra makes two key contributions

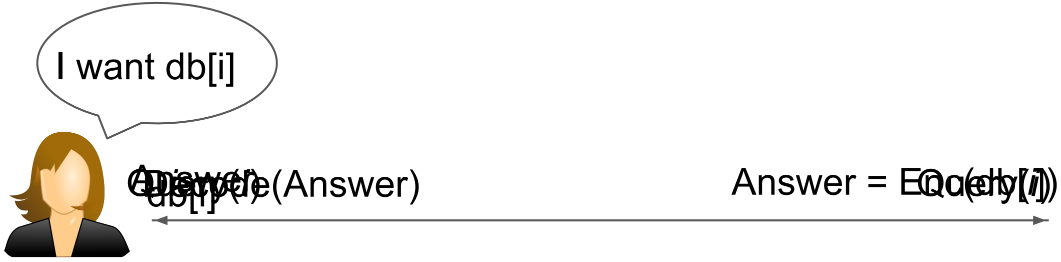
Challenge 1: Unlinking the caller and callee

Solution 1: A novel communication architecture exploiting Private Information Retrieval (PIR)

Challenge 2: Scaling with low latency

Solution 2: A new PIR scheme with faster processing time

A brief background on Private Information Retrieval



Client

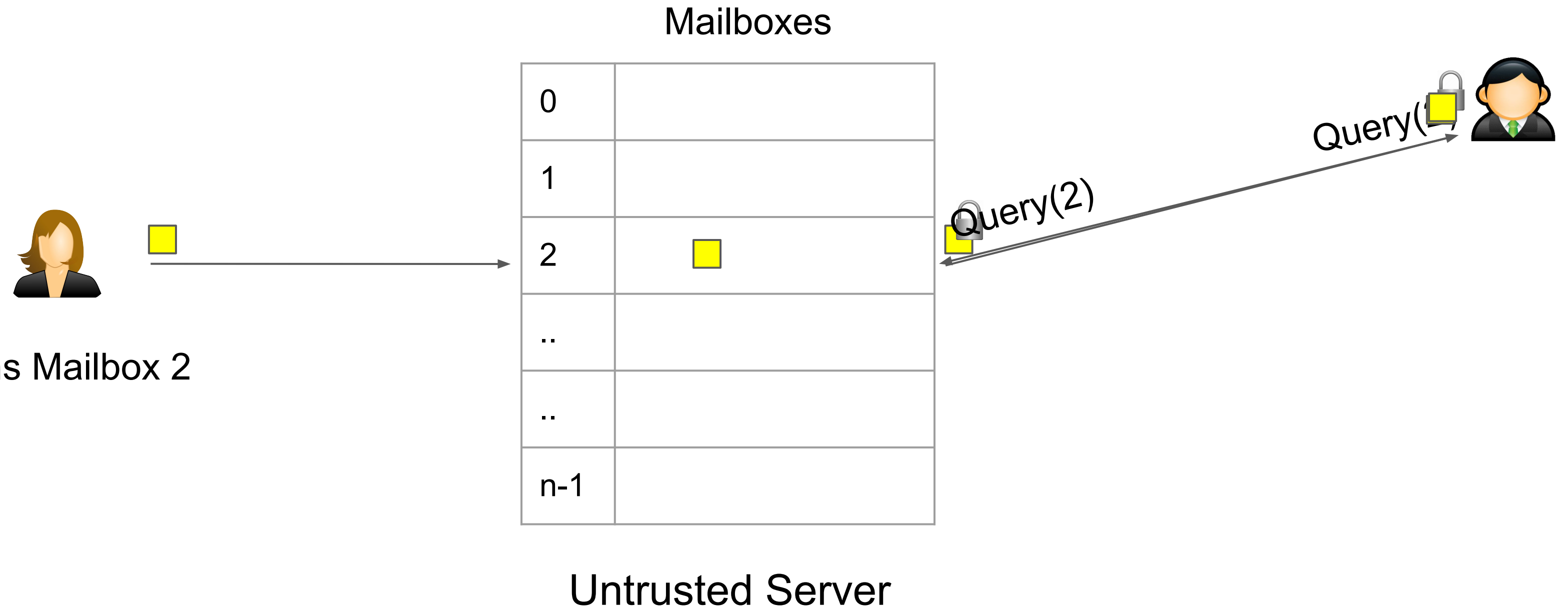
	db
0	01011001010101001010 10
1	01110001010101001010 10
2	10011001010101001010 10
.	11011001010101001010 10
.	01011011010101001011 10
n - 1	01101001110101101010 10

Untrusted Server

Addra’s architecture

Challenge 1: Unlinking the caller and callee

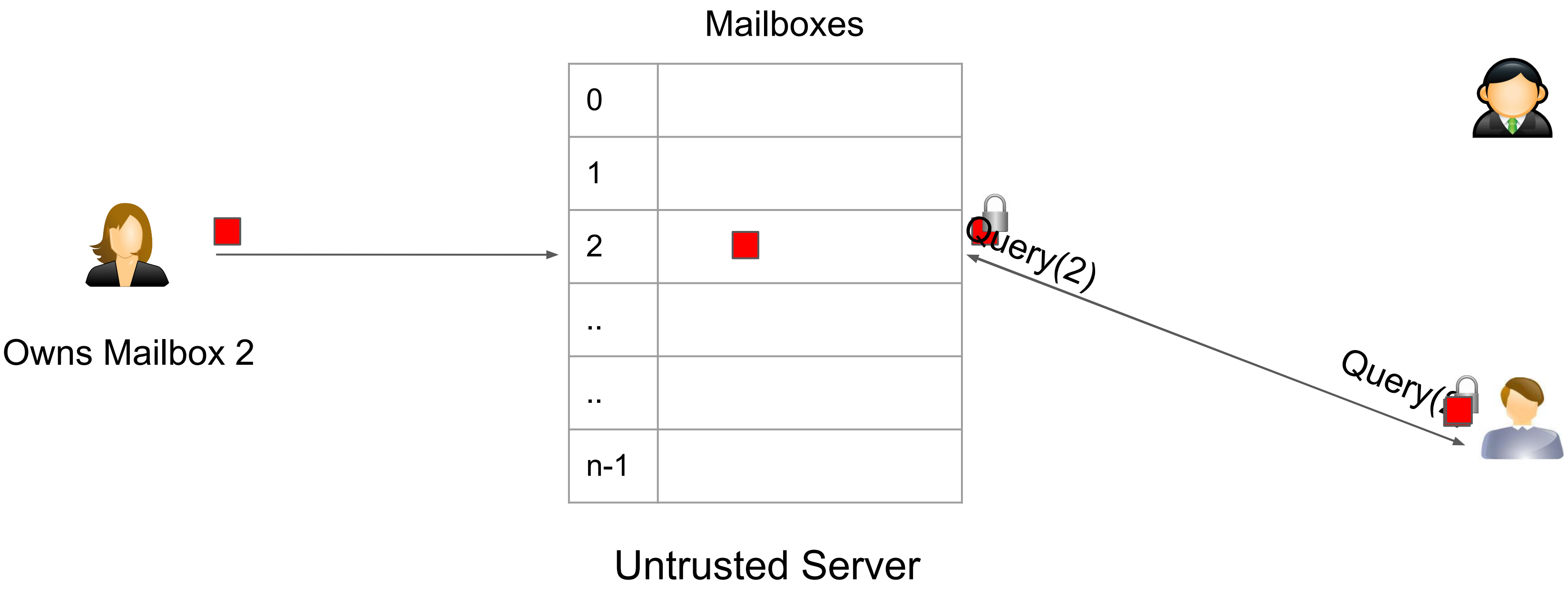
Solution 1: A novel communication architecture exploiting Private Information Retrieval (PIR)



Addra’s architecture

Challenge 1: Unlinking the caller and callee

Solution 1: A novel communication architecture exploiting Private Information Retrieval (PIR)



Mailboxes

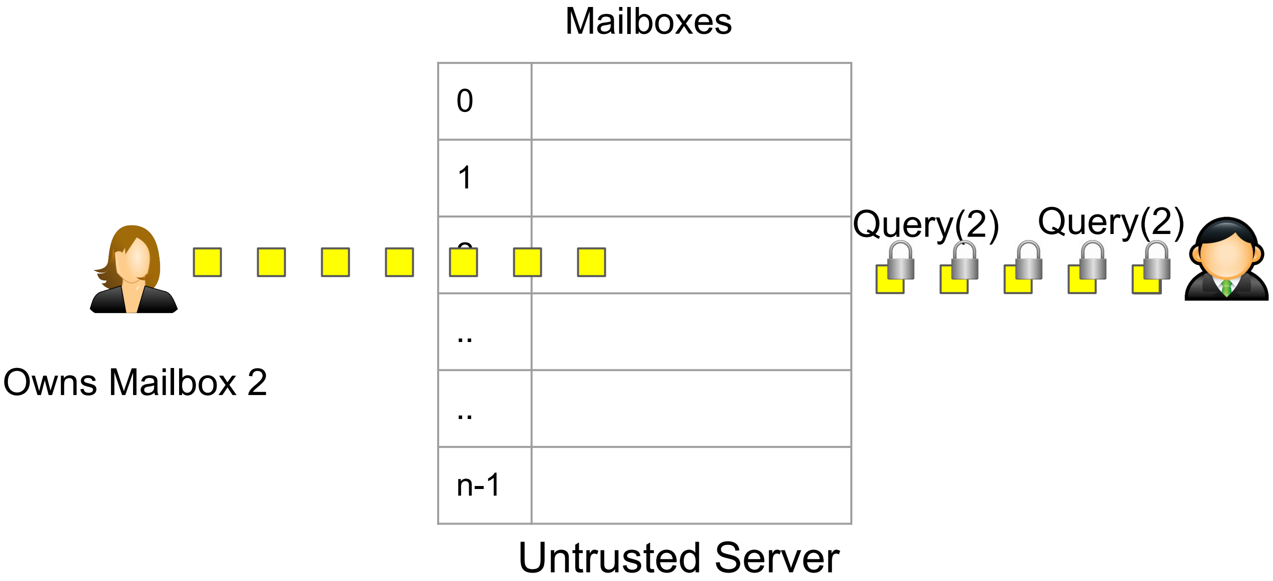
0	
1	
2	🟥
..	
..	
n-1	

Owns Mailbox 2

Untrusted Server

The simple architecture provides advantages for voice call

1. Query can be reused over the entire call



Mailboxes

0

1

2

..

..

n-1

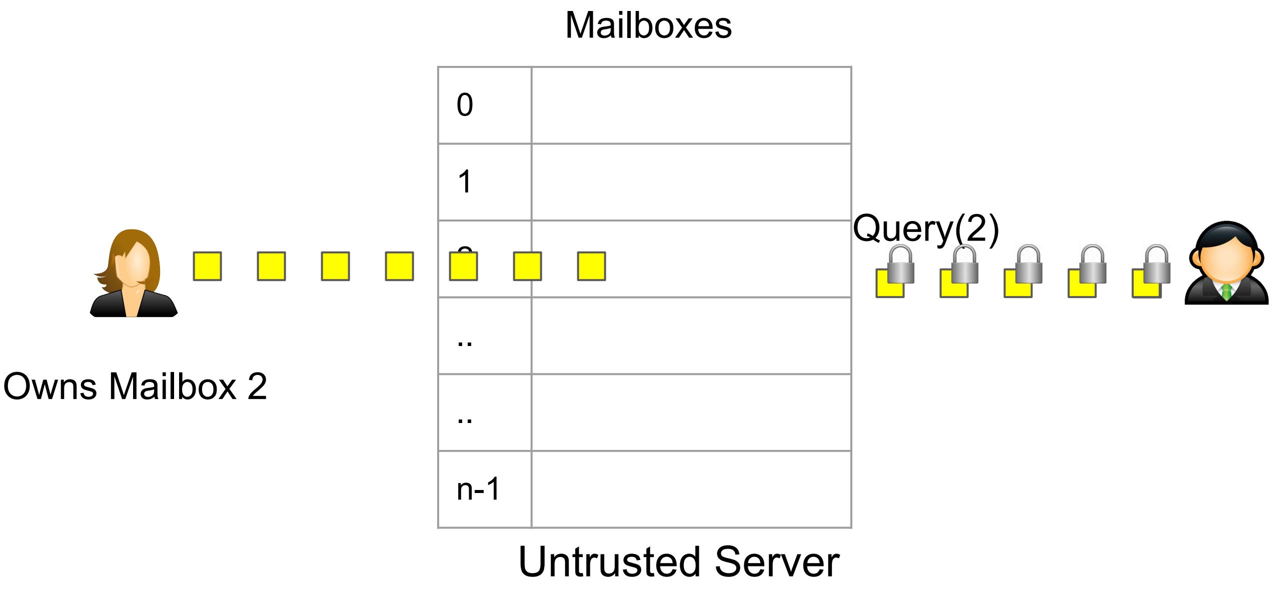
Query(2) Query(2)

Owns Mailbox 2

Untrusted Server

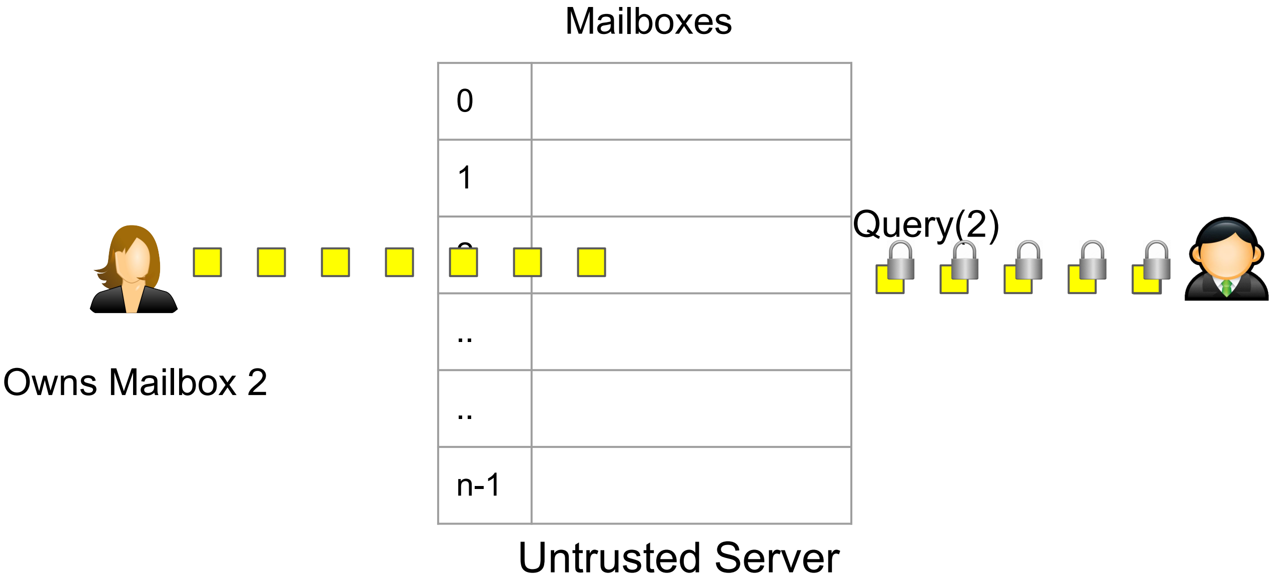
The simple architecture provides advantages for voice call

1. Query can be reused over the entire call



The simple architecture provides advantages for voice call

1. Query can be reused over the entire call



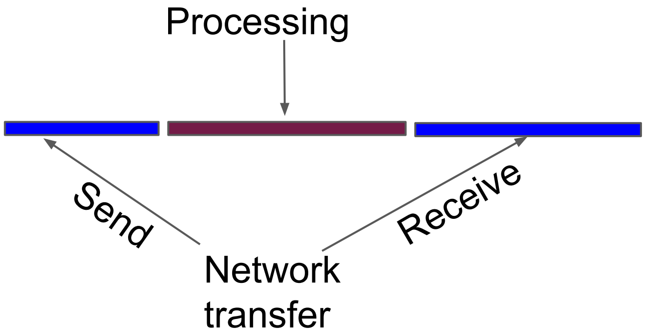
2. A voice packet can be transferred in two hops

A new PIR scheme: FastPIR

Challenge 2: Scaling with low latency

Solution 2: A new PIR scheme with faster processing time

Latency breakdown



Existing PIR schemes:

- XPIR [PETS ’16]
- SealPIR [S&P ’18]

Trade off between processing and receive time!

FastPIR

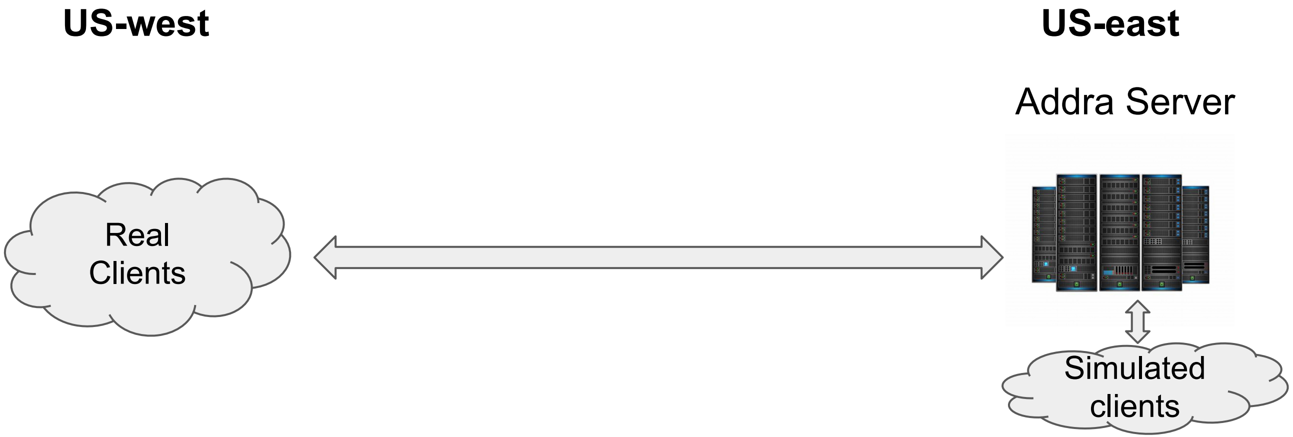
- Faster than both XPIR and SealPIR
- Small response size

Details available in our paper.

Evaluation

- What is Addra’s latency performance?

Setup



US-west

Real Clients

US-east

Addra Server

Simulated clients

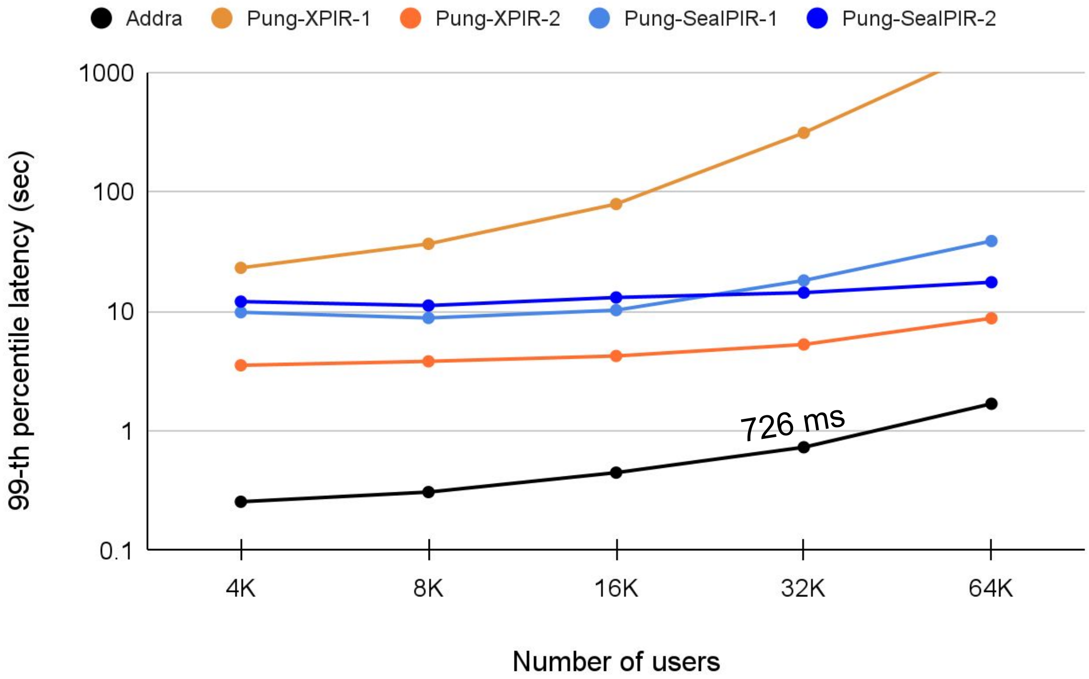
Baseline: 2 variants of Pung

- Pung-XPIR [OSDI ’16]
- Pung-SealPIR [S&P ’18]

Evaluation

- What is Addra's latency performance?

End-to-end latency



7x better than the best Pung variant

Evaluation

- How does FastPIR compare to XPIR and SealPIR?

Setup: 1M elements, 256 bytes each

PIR Scheme	Processing time (ms)	Response size (KB)
FastPIR	947	64
XPIR-1	3,389	32
XPIR-2	1,894	288
SealPIR-1	76,216	32
SealPIR-2	2,556	320

Faster than all variants!

Key takeaways from the talk

- Hiding voice call metadata is crucial for privacy
- Addra can hide voice call metadata with two key techniques:
  - A new mailbox architecture
  - A new PIR scheme FastPIR
- Addra can support 32K users with 726ms message latency

Thank You!

Ishtiyaque Ahmad
Ishtiyaque@ucsb.edu

Addra:https://github.com/ishtiyaque/Addra
FastPIR: https://github.com/ishtiyaque/FastPIR