Talek: Private Group Messaging with Hidden Access Patterns

Raymond Cheng
Will Scott, Elisaweta Masserova, Irene Zhang,
Vipul Goyal, Arvind Krishnamurthy,
Tom Anderson, Bryan Parno

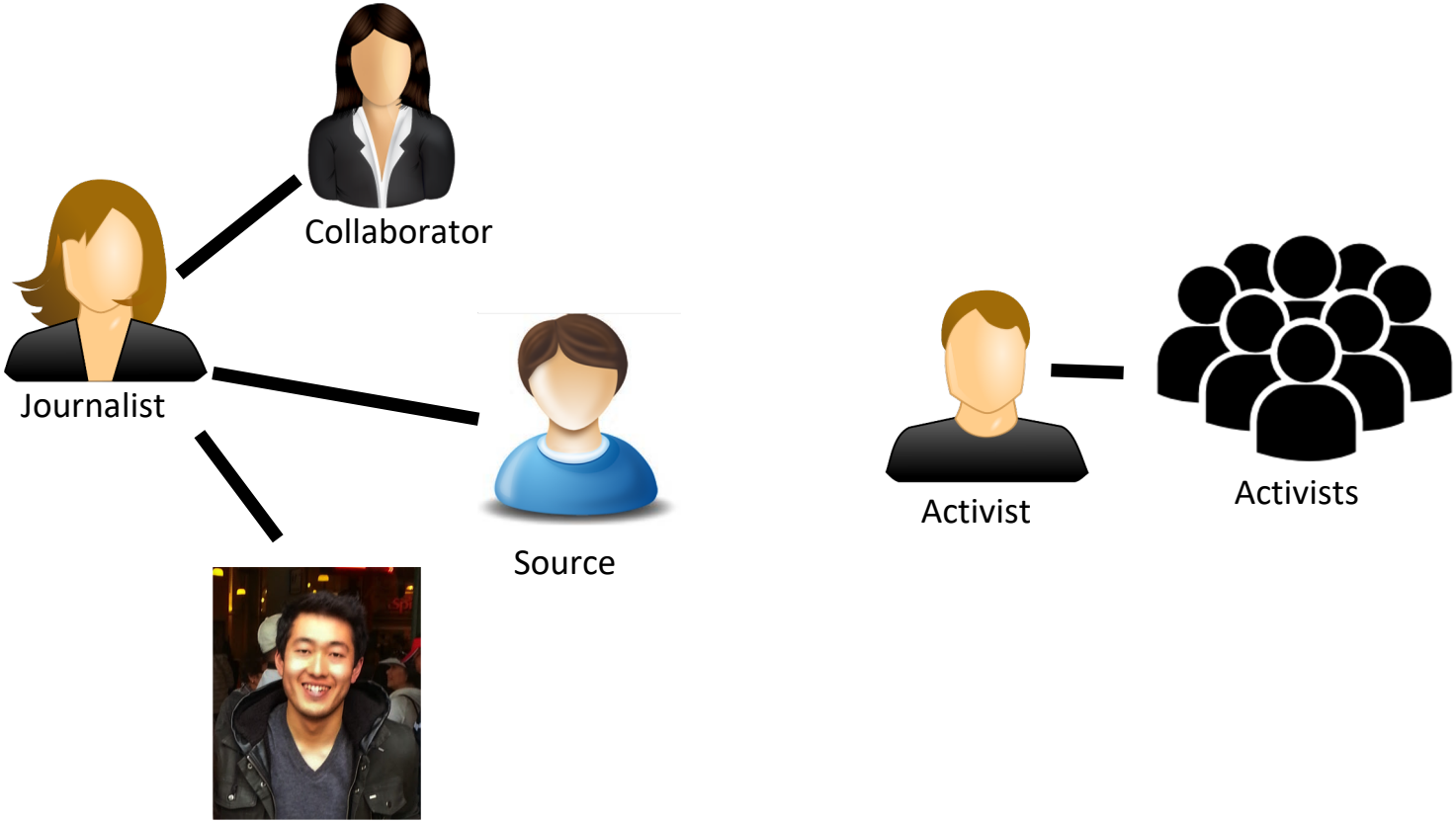
Group Messaging

Chat	Newsfeed	Calendar	Game	IoT
1:message	1: image	1: new event	1: playerA move	1: config lights
2:message	2: tweet	2: delete event	2: playerB move	2: security video
3:message	3: video	3: update	3: playerA move	3: set temp

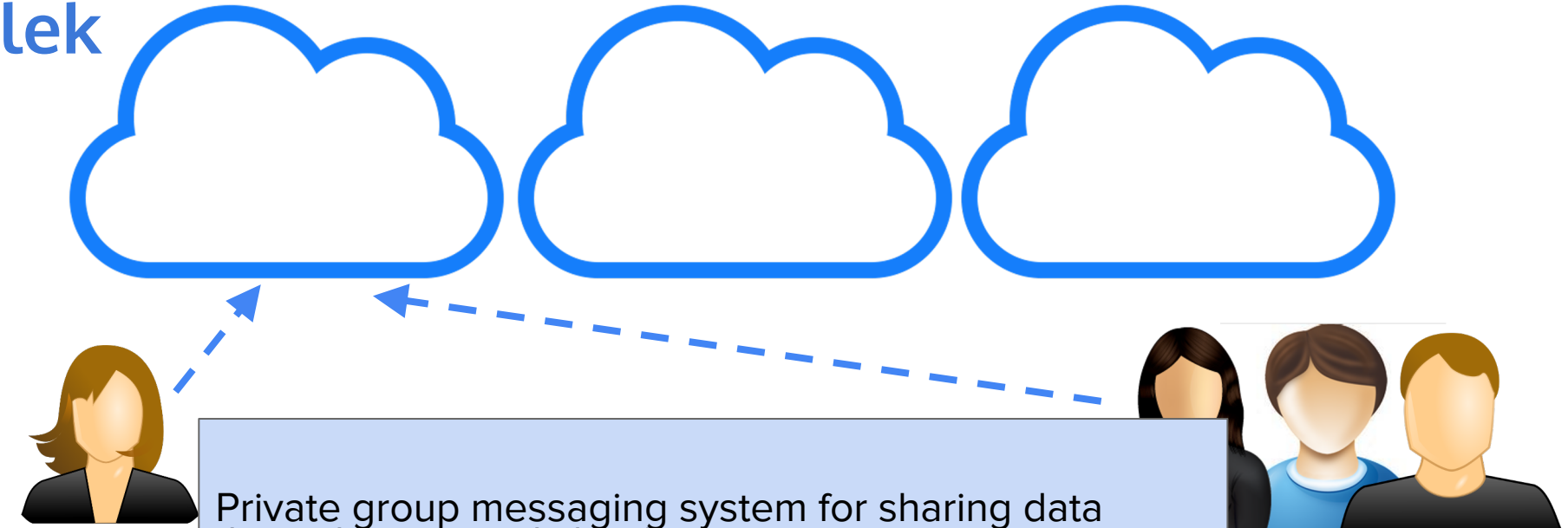
Encryption protects the content…

Chat	Newsfeed	Calendar	Game	IoT
1:message	1: image	1: new event	1: playerA move	1: config lights
2:message	2: tweet	2: delete event	2: playerB move	2: security video
3:message	3: video	3: update	3: playerA move	3: set temp

… but communication patterns are exposed



Talek



Private group messaging system for sharing data through untrusted clouds

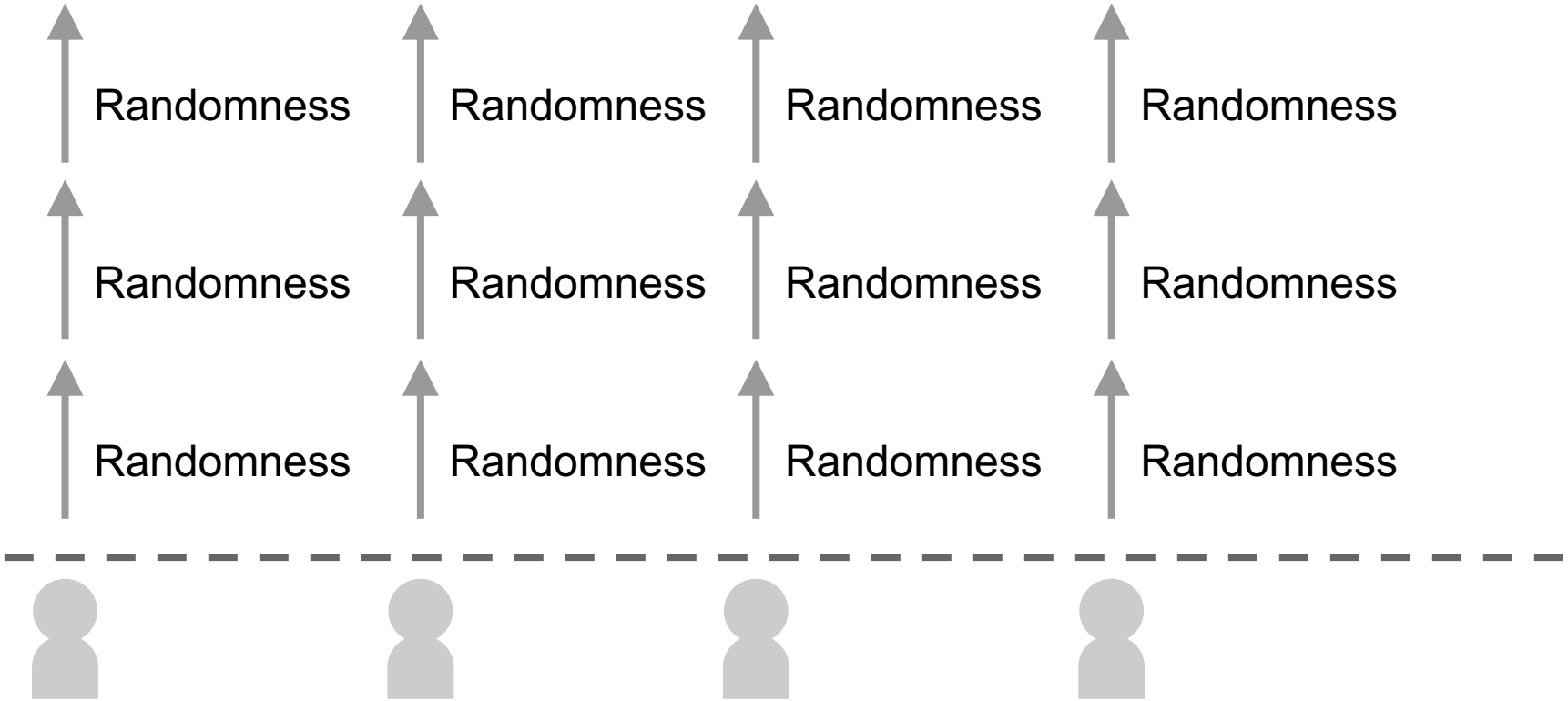
- Hide both contents and communication patterns
- Made practical using ***oblivious logging*** and ***private notifications***
- System with 3-4 orders of magnitude better performance than closest related work

Security Goal: Indistinguishability

Any two access sequences from a client look indistinguishable to the adversary

Security Goal: Indistinguishability

Any two access sequences from a client look indistinguishable to the adversary



Talek Related Work

System	Security Goal	Threat Model	Technique	Application
Talek	indistinguishability	≥1	IT-PIR	pub/sub
Pynchon Gate	k-anonymity	≥1	mixnet/IT-PIR	email
Riffle	k-anonymity	≥1	mixnet/IT-PIR	file-sharing
Riposte	k-anonymity	≥1	IT-PIR	broadcast
Dissent	k-anonymity	≥1	DC-nets	broadcast
Vuvuzela	differential privacy	≥1	mixnet	1-1 messaging
DP5	indistinguishability	≥1	IT-PIR	chat presence
Popcorn	indistinguishability	≥1	C-PIR/IT-PIR	video streaming
Pung	indistinguishability	0	C-PIR	key-value store
ORAM	indistinguishability	0	ORAM	storage

Weaker Security Goal

Application Specific

Prohibitively Expensive

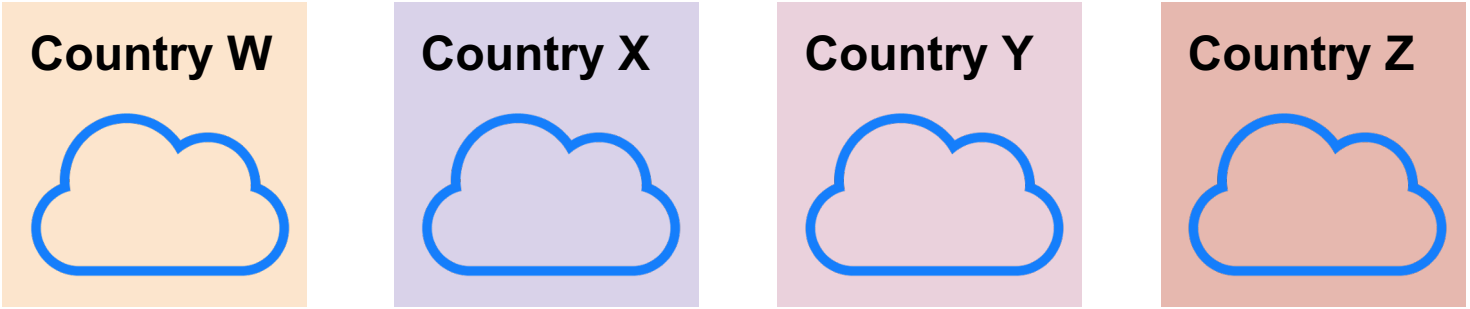
Talek Goals

Security Goal: Indistinguishability
Any two access sequences from a client look indistinguishable to the adversary

Systems Goals:

- Mobile-friendly: 1 message per request/response
- Efficient: Thousands of online users sending a message every 5 seconds
- General Purpose: messaging and newsfeeds
- Low latency: ~5-10s

Anytrust Threat Model

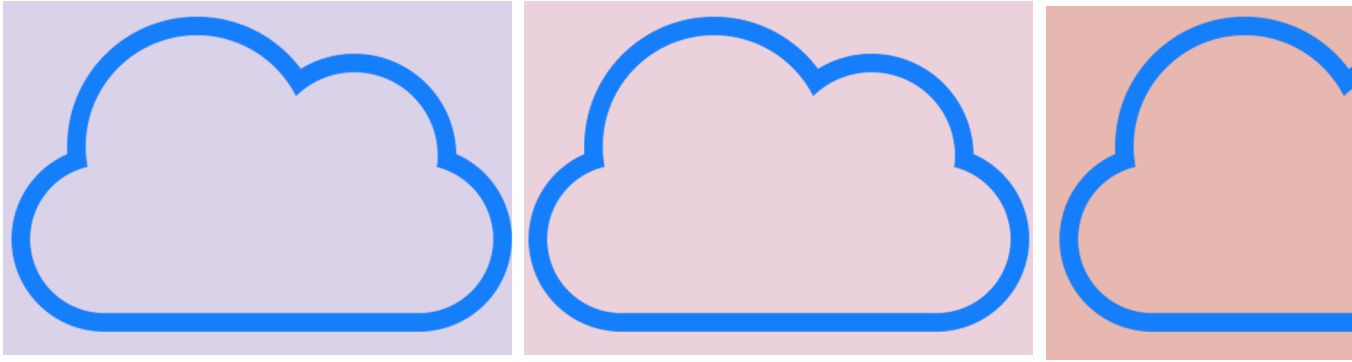


- Application configured with >1 independent clouds
- Clouds logging everything about users

At least 1 non-colluding

Talek Threat Model

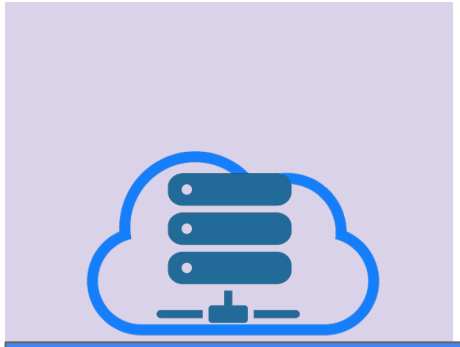
Trusted groups

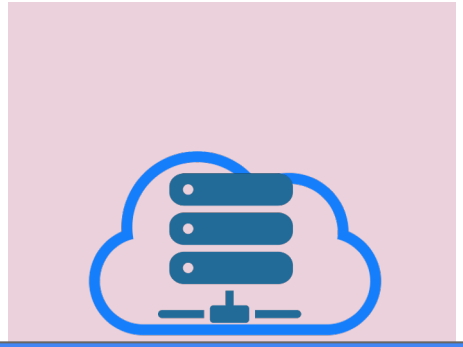


Anytrust: At least 1 non-colluding

Mutually distrusting users

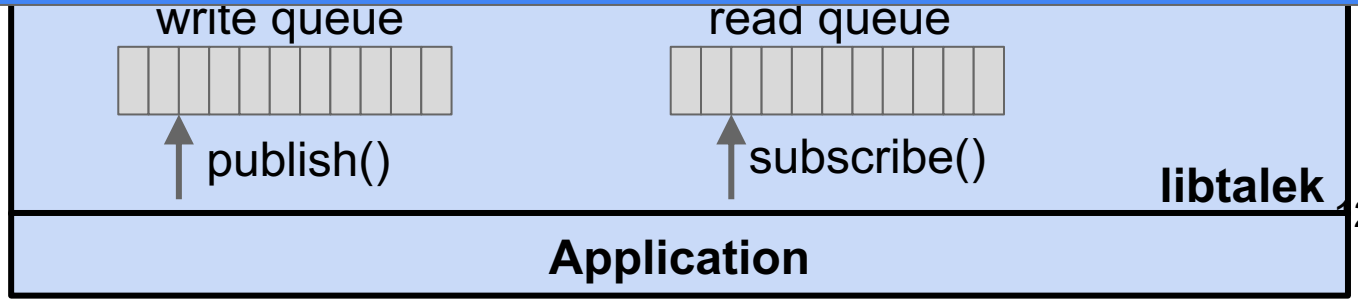
Talek Overview



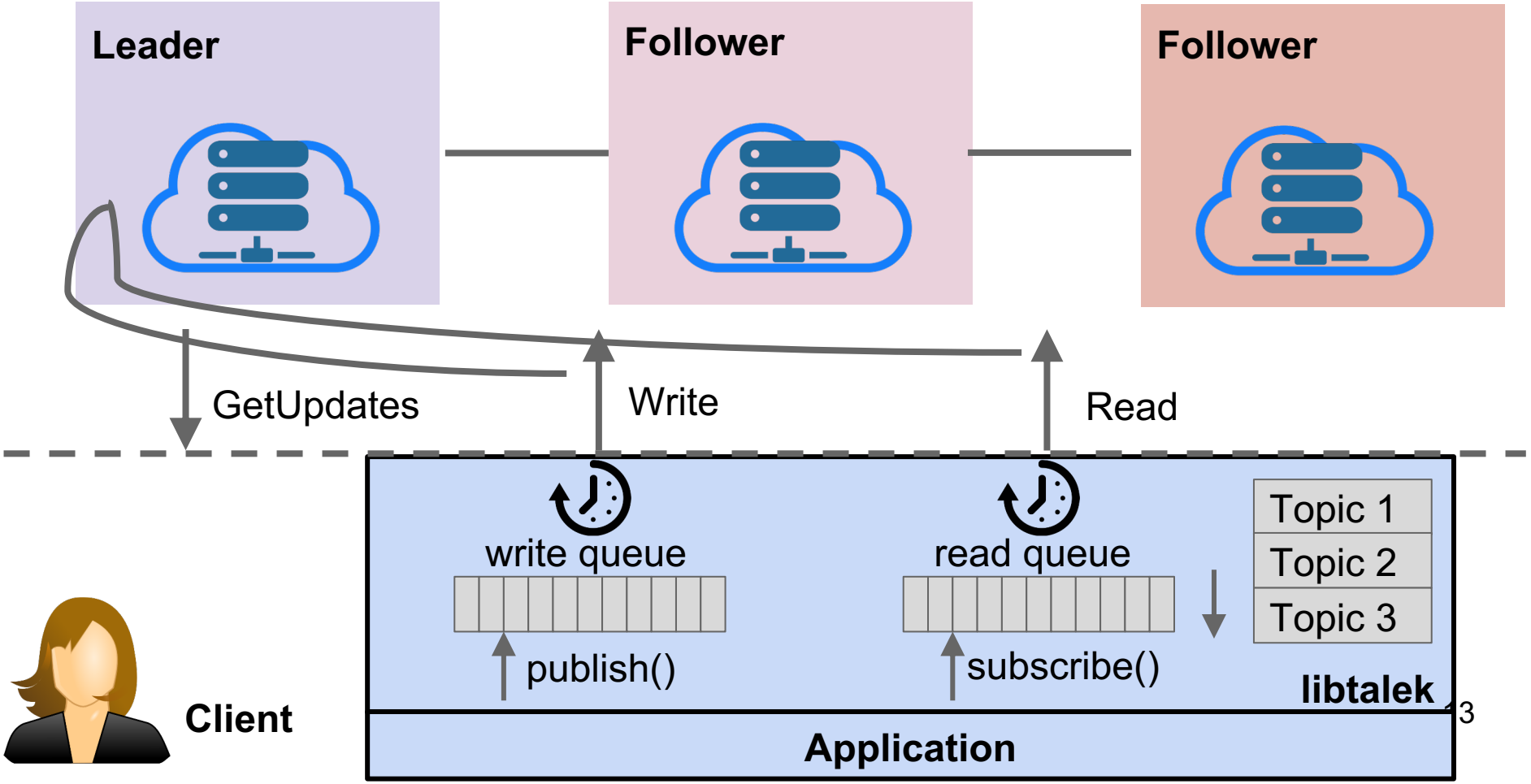


Oblivious logging enables servers to operate on noise, while delivering group messaging functionality

Client



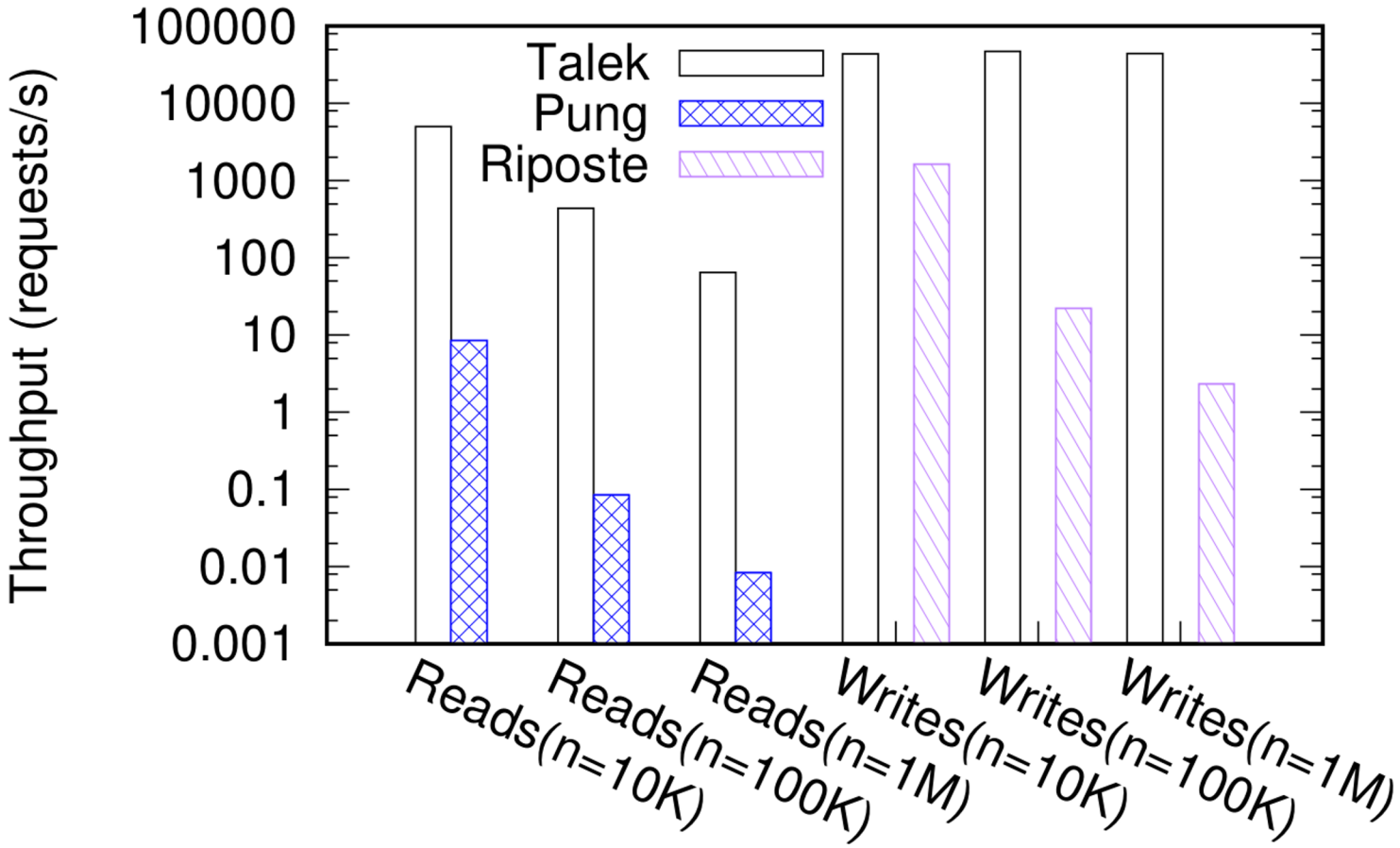
Talek Overview



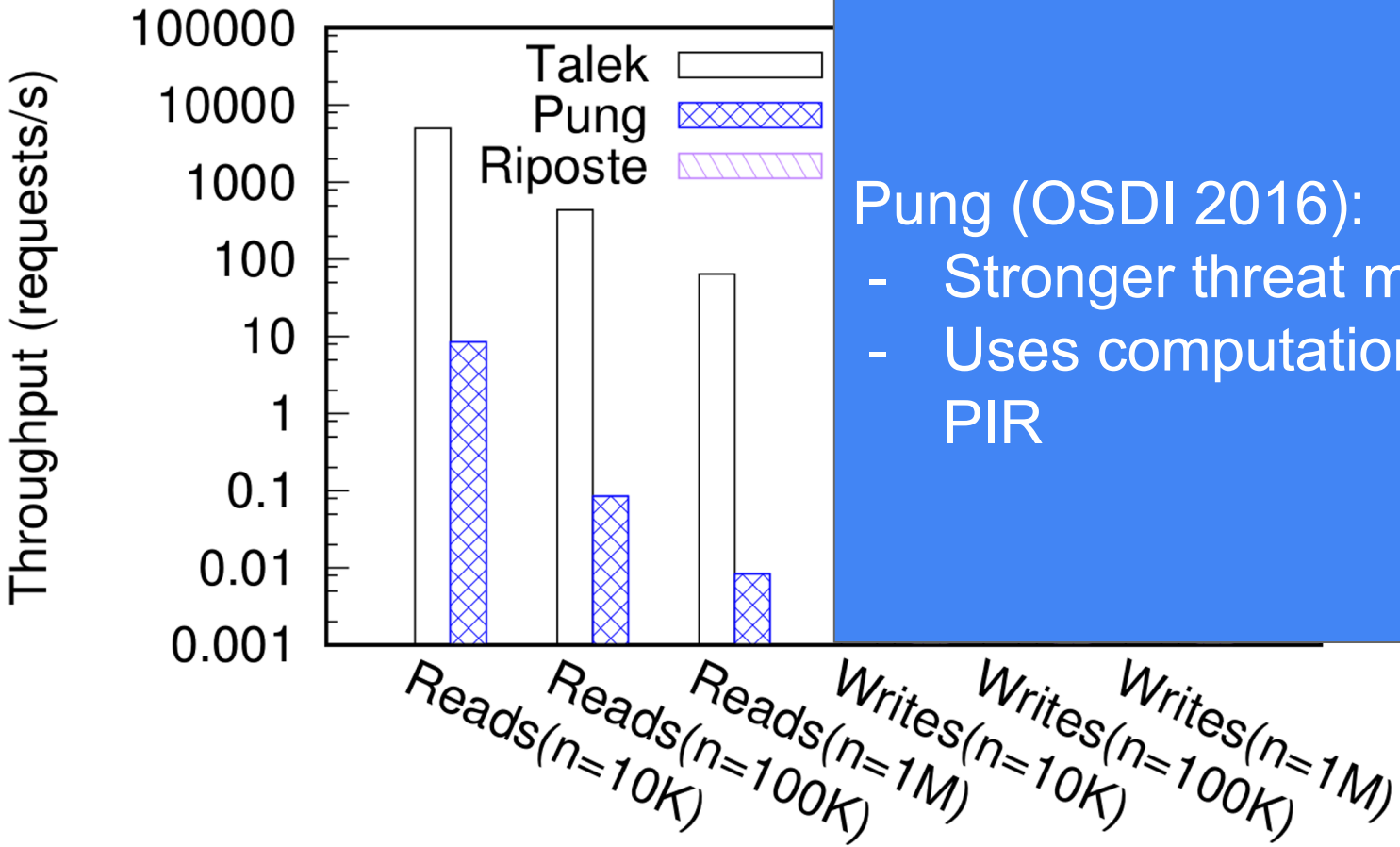
Oblivious Logging

1. How do we bound the cost of a PIR operation?
2. How do publishers write in a way that looks random?
3. How do subscribers find messages on the server?
4. How do we deal with write conflicts?
5. How do we keep all servers consistent?

Comparison to Previous Work



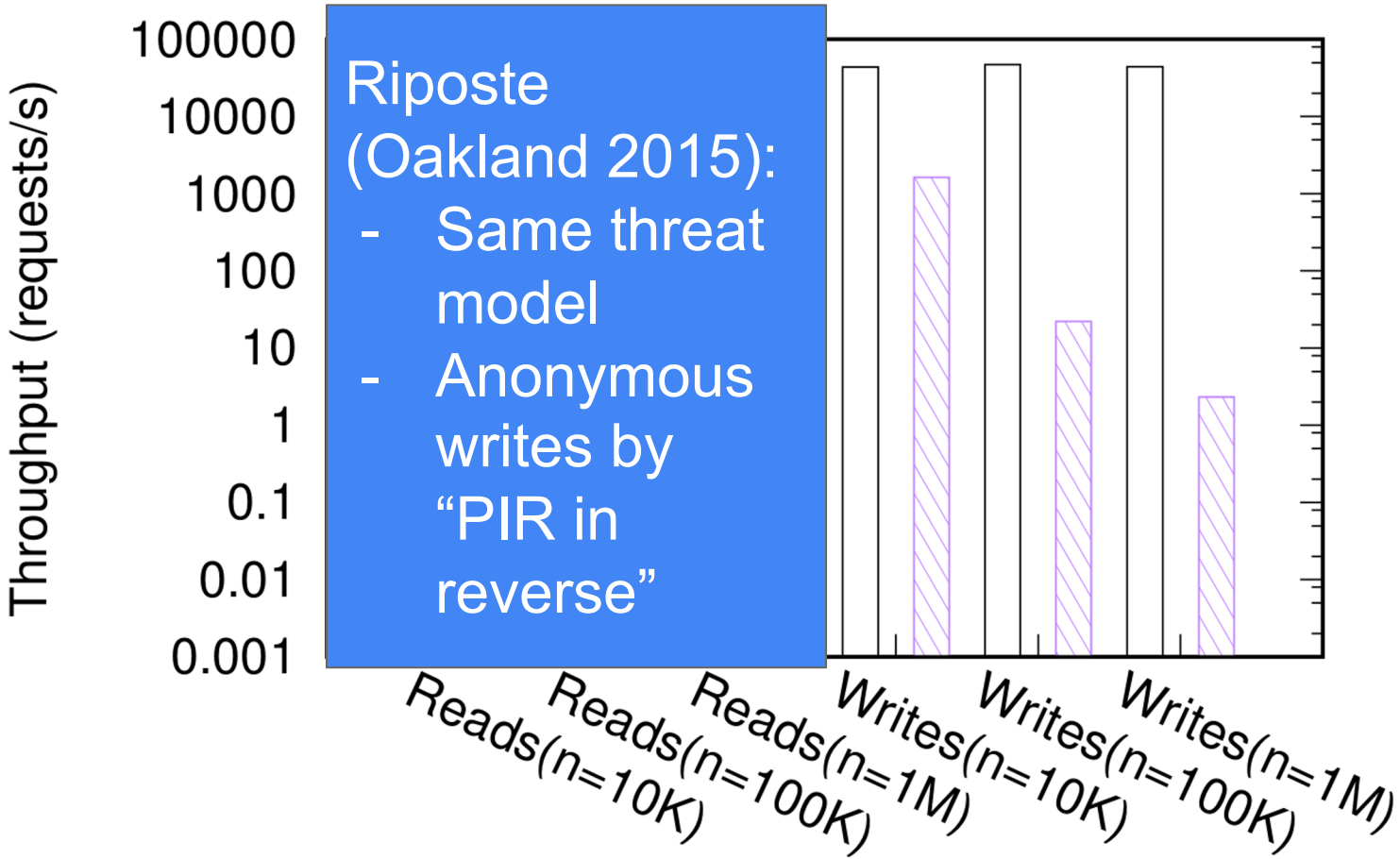
Comparison to Previous Work



Pung (OSDI 2016):

- Stronger threat model
- Uses computational PIR

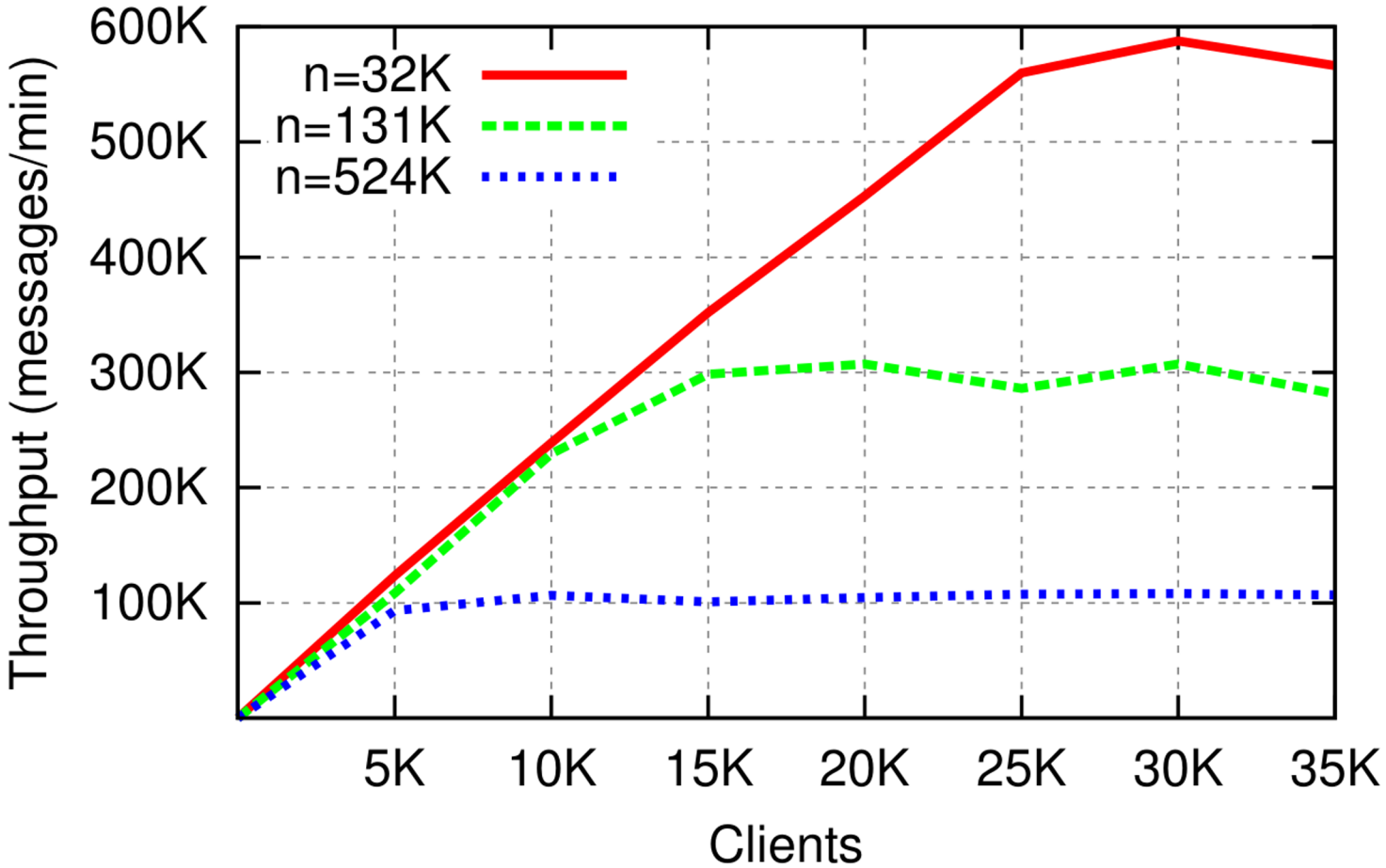
Comparison to Previous Work



Riposte (Oakland 2015):

- Same threat model
- Anonymous writes by "PIR in reverse"

Scaling Clients



privacylab / talek

Watch 4 | Star 4 | Fork 0

Code | Issues 26 | Pull requests 0 | Projects 0 | Pulse | Graphs

a Private Publish Subscribe System

privacy cloud pubsub publish-subscribe messaging anonymity

316 commits | 1 branch | 0 releases | 2 contributors

Branch: master | New pull request | Find file | Clone or download

ryscheng committed on GitHub Merge pull request #51 from privacylab/serverrefactor ... Latest commit 17d444b 4 hours ago

benchmark	trust domain vs server address in frontend RPC.	5 days ago
bloom		19 days ago
cli		5 hours ago
common		a day ago
cuckoo		4 days ago
drbg		4 days ago
libtalek		4 days ago
pir	fix linting on pir, bloom	19 days ago
pird	adding some deps for flags	2 days ago
server	PR updates	5 hours ago
vendor	gnu-style flags and setting with envrionment variables	a day ago
.gitignore	adding some deps for flags	2 days ago
.travis.yml	add coverage reporting to travis	4 days ago

https://github.com/privacylab/talek

me@raymondcheng.net