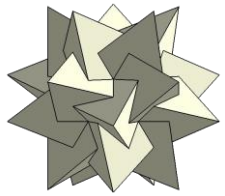
Contact: Dr. Rafail Ostrovsky, rafail@stealthsoftwareinc.com



Function Secret Sharing for PSI-CA: With Applications to Private Contact Tracing

Speaker:

Steve Lu, CEO, Stealth Software Technologies, Inc.

Contact: steve@stealthsoftwareinc.com

Joint Work with:

Samuel Dittmer Yuval Ishai Rafail Ostrovsky

kryptowire

Mohamed Elsabagh Nikolaos Kiourtis Brian Schulte Angelos Stavrou

NIST Workshop on Challenges for Digital Proximity Detection in Pandemics: Privacy, Accuracy, and Impact
January 26-28, 2021

This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA). This work was supported by DARPA and NIWC Pacific under contract N66001-15-C-4065 and by DARPA, AFRL/RIKD,USAF, and AFMC under FA8750-18-C-0054. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes not withstanding any copyright notation thereon. The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

Intro

Our Approach

- **We describe new methods of increasing accuracy and privacy in decentralized contact tracing**

- **Key insight**
  - **Accuracy: Context-aware risk score attached to tokens**
  - **Robustness: Hash location+time with token in TEE for hardening against malicious context attacks**
  - **Privacy: New cryptographic protocol that hides infected tokens and only reveals weighted risk score**

mSense App – Decentralized Contact Tracing with Extensions

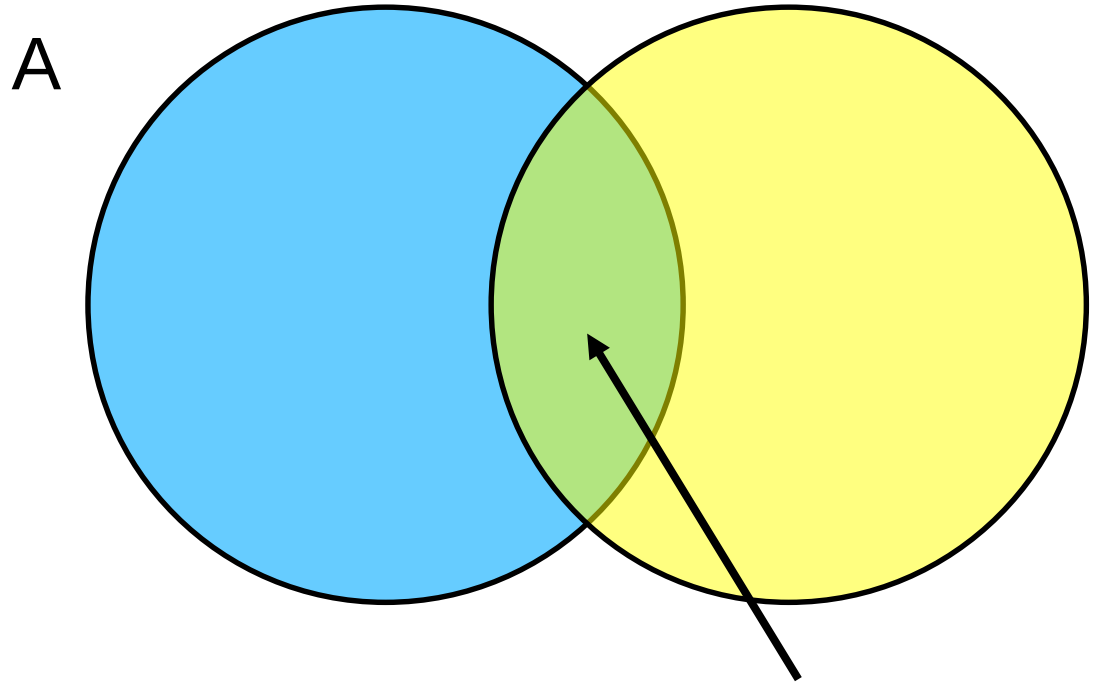
Key Innovations	High Level System Requirements
1. Tracking risk of infection; not tracking people •Does NOT expose all contacts •Does expose probable exposure	1.High Accuracy
2.Hardware proximity sensing and geolocation •Edge anonymization for data at rest and in transit •Server-side cryptographic calculations on anonymized users and locations	2.High Scalability
3.Fully encrypted database AND computation •Fast updates with parallel scaling •Data, queries, and responses are ALL encrypted; including from servers	3.Strong Privacy
	4. Robustness

		Centralized [TraceTogether,...]	Decentralized [D3-PT, Apple/Google, PACT,...]	Epione [TSS+20]	CleverParrot [CKL+20]	**This Work [mSense/ PSI-WCA]**
Servers	Trusted Server	Yes	No	No	No	No
	Number of Servers	1	1	2	1	2
Privacy	Social Graph					
	Server					
	User-to-user					
Robustness Against	Relay					
	Replay					
	Upload Omission				Feature	
	Trace Omission					

		Centralized [TraceTogether,...]	Decentralized [D3-PT, Apple/Google, PACT,...]	Epione [TSS+20]	CleverParrot [CKL+20]	**This Work [mSense/ PSI-WCA]**
Tracing Cost	User to Server Comm	O(n)	N/A	O(n log N)	N/A	O(nk)
	Server to User Comm	O(1)	O(N)	O(n)	O(N')	O(1)
	User Crypto Work	N/A	Non-crypto O(N) match	O(n) asym	O(N') asym	O(n) sym
	Server Crypto Work	Non-crypto match	N/A	O(nN) asym	N/A	O(N) sym
	Rounds	1	0.5	2	0.5	1
Result	Result Returned	Yes/No	All "infected tokens"	Count of exposures	Tokens of exposures	Weighted risk score
Underlying Crypto	Primary Crypto Tools	Central trust	PRF-style "PSI"	DH-style PSI-CA plus 2PIR	DH-style PSI	PSI-(W)CA from FSS

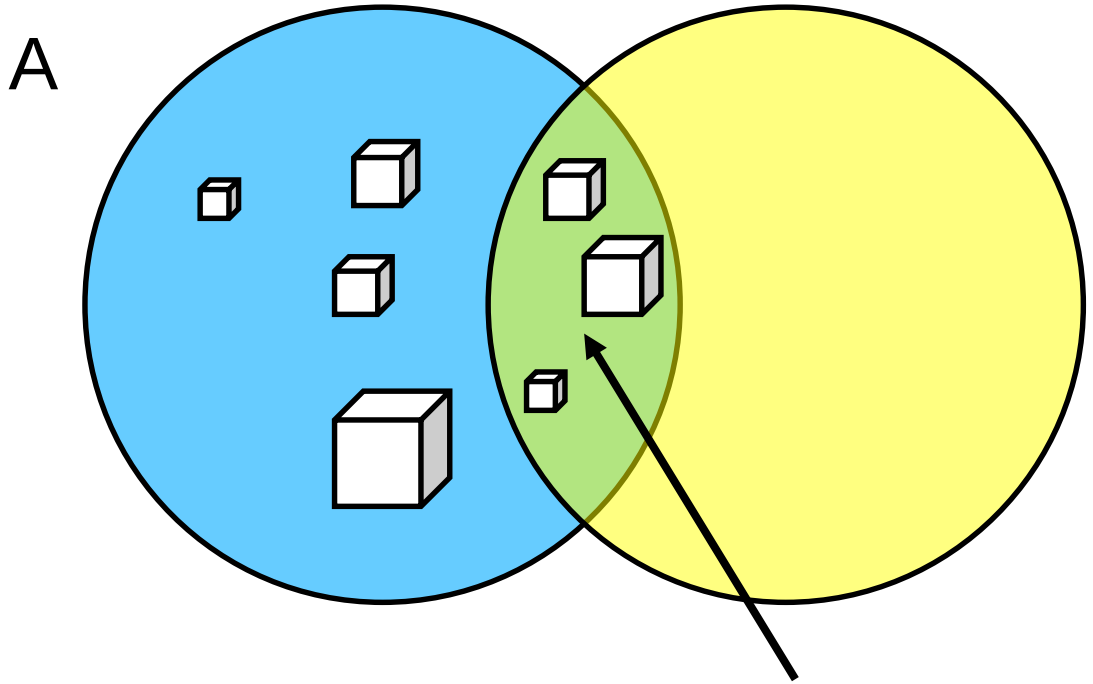
Private Set Intersection

Private Set Intersection [M86, HFH99, FNP04, KS04, FIPR05,...]



Reveal only the intersection, hide non-intersected data

Private Set Intersection – Weighted Cardinality (PSI-WCA)



Reveal only the size intersection, hides the intersection and non-intersected data

A = Set of tokens I've received + mSense weights

B = Set of tokens of infected individuals

PSI-WCA provides weighted risk score!

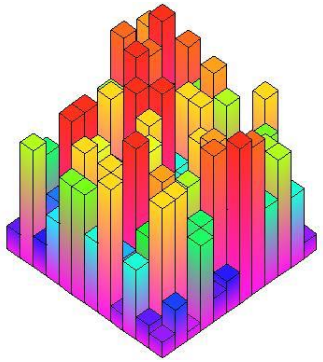
Putting It Together

This work: Building PSI-(W)CA From Function Secret Sharing

What is Function Secret Sharing [GI14, BGI15, BGI16,...]?

- Crypto protocol to split a function F into F_1 and F_2 such that $F_1(x)+F_2(x) = F(x)$ and individually F_1, F_2 reveal nothing about F

Theorem [GI14]: Sharing a point function P can be done using only symmetric-key crypto (e.g. AES)



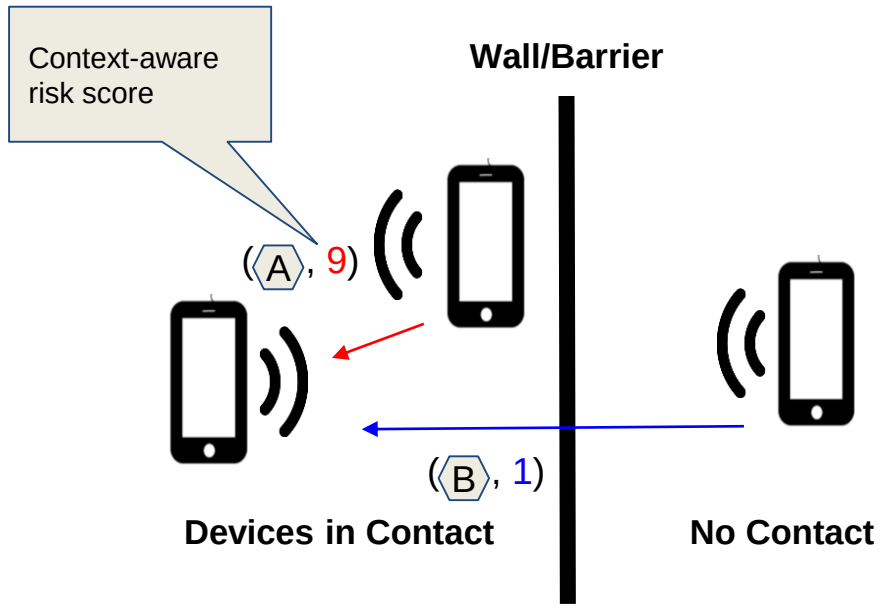
$$P(x) = \begin{cases} b \text{ if } x=a \\ 0 \text{ otherwise} \end{cases}$$

Token

Weight

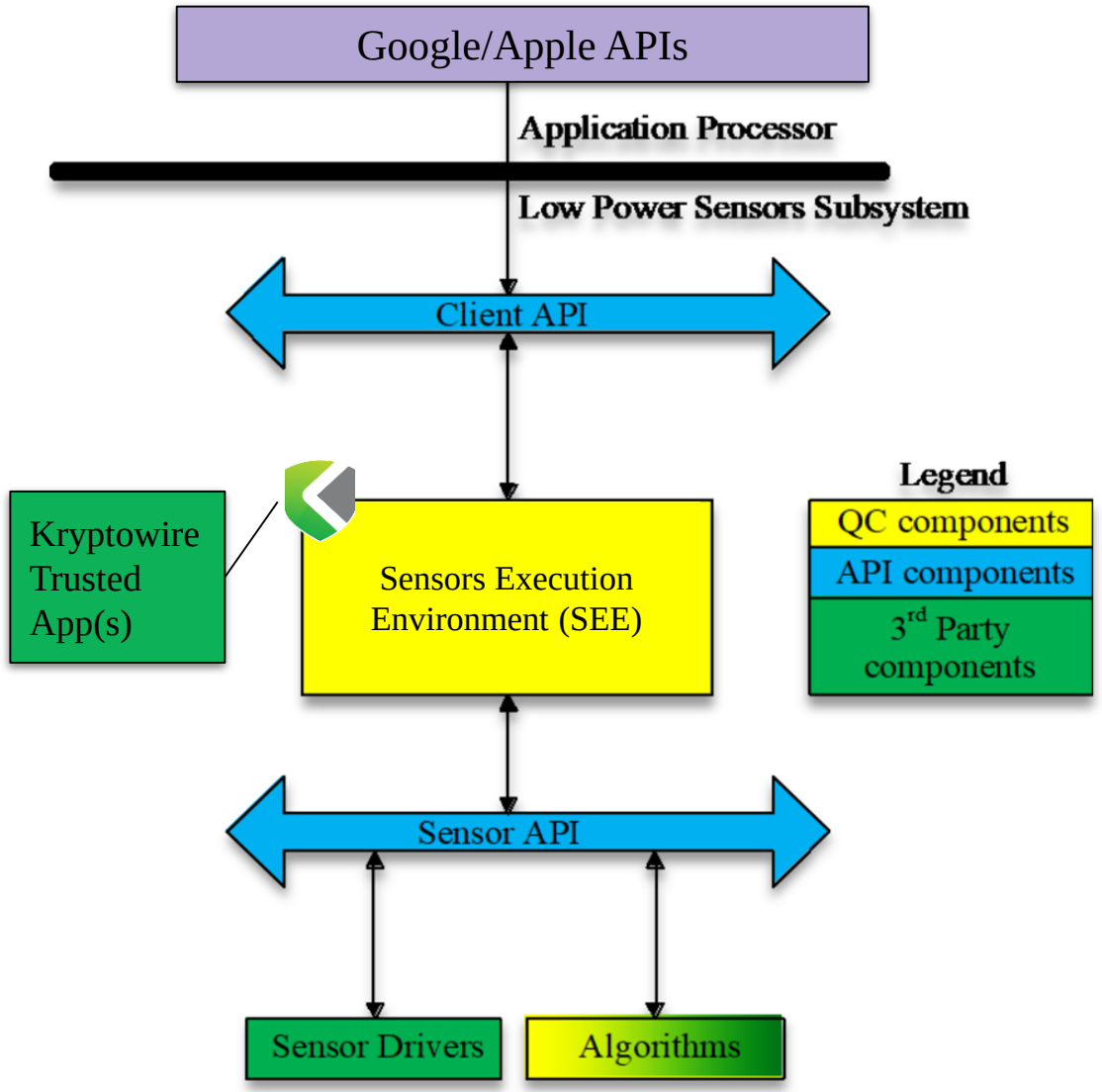
Situational Accuracy

- Improved sensor timings via chipset level access and experience
- Use of additional modalities to establish trusted location, sensor assisted positioning for more accurate location
- Utilize APIs to perform barrier detection (WiFi, Audio, etc)
- Context detection and baselining



Sensory Accuracy

- Access to the chipset level sensing environments with raw sensor data to assist in correcting for differences across APIs & Devices
- Chipset level applications work on wearables & mobile phones
- Access to raw sensory data and ability to load custom fusion algorithms



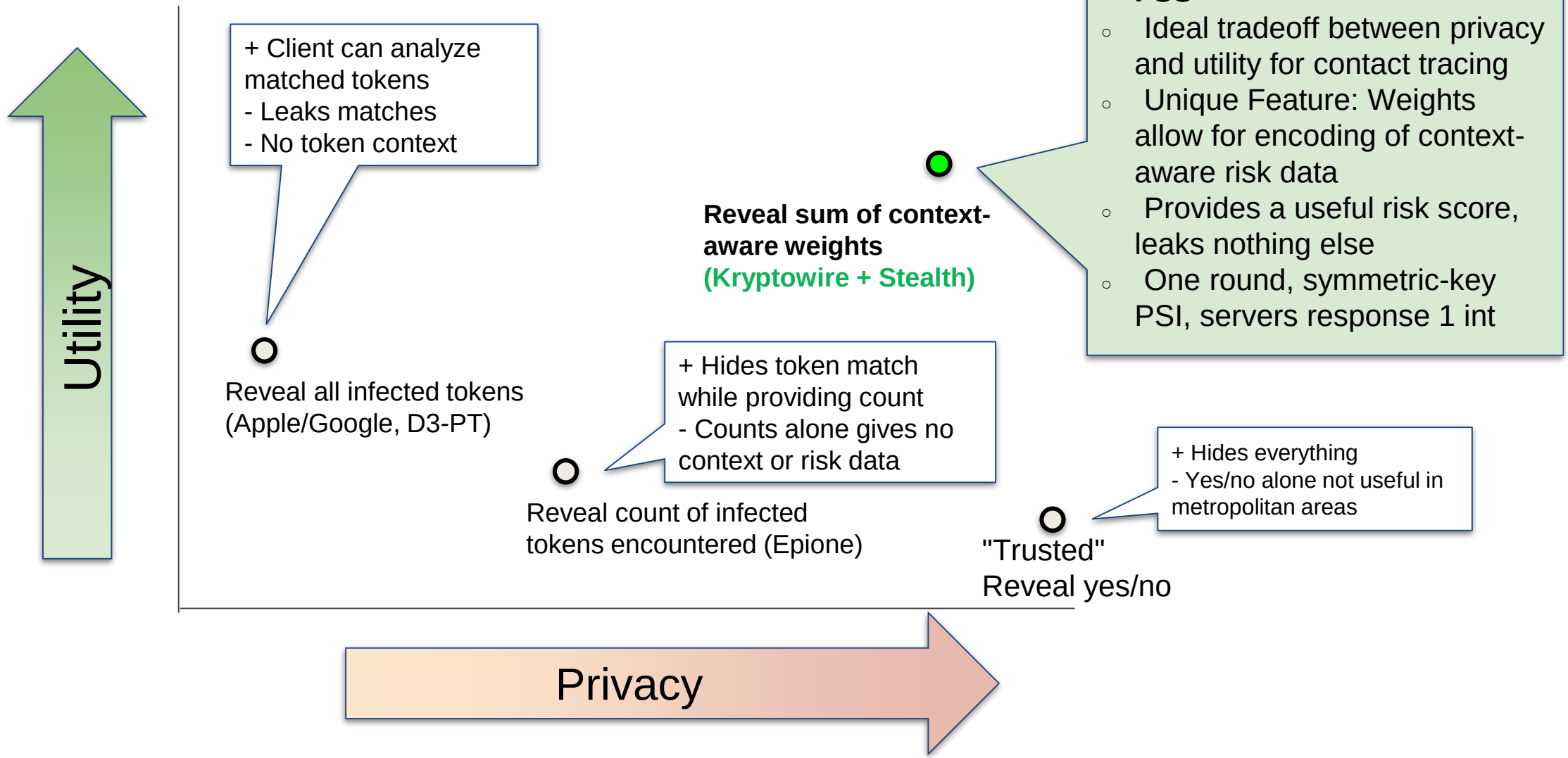
Building PSI-(W)CA From Function Secret Sharing

- For each token a_i, phone splits P_i into $P_{i,1}$ and $P_{i,2}$, sends each $P_{i,b}$ to server b (two servers)
  - Split server model has a long theoretical history (e.g. [CGKS95]) and recently used to great effect in practical privacy technologies (e.g [Prio])
- Each server b computes sum over all N infected tokens y_j, all n phone splits P_i:

$$\text{response}_\text{b} = \sum_{i=1}^{n} \sum_{j=1}^{N} P_{i,b}(y_j)$$

Sum of the responses = weighted risk score!

- Naïve computation is O(nN), we also use careful combinatorial hashing to reduce server work


Utility
+ Client can analyze matched tokens
- Leaks matches
- No token context
Reveal all infected tokens (Apple/Google, D3-PT)
+ Hides token match while providing count
- Counts alone gives no context or risk data
Reveal count of infected tokens encountered (Epione)
+ Hides everything
- Yes/no alone not useful in metropolitan areas
"Trusted" Reveal yes/no
Reveal sum of context-aware weights (Kryptowire + Stealth)
• Tech: Private Set Intersection - Weighted Cardinality (PSI-WCA) via FSS
◦ Ideal tradeoff between privacy and utility for contact tracing
◦ Unique Feature: Weights allow for encoding of context-aware risk data
◦ Provides a useful risk score, leaks nothing else
◦ One round, symmetric-key PSI, servers response 1 int
Privacy

Thank You!

Paper

arXiv: https://arxiv.org/abs/2012.13053