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
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/RKID, 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
• 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

<table>
<thead>
<tr>
<th>Key Innovations</th>
<th>High Level System Requirements</th>
</tr>
</thead>
</table>
| 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 |
<p>|                     | 4. Robustness |</p>
<table>
<thead>
<tr>
<th></th>
<th>Centralized [TraceTogether,...]</th>
<th>Decentralized [D3-PT, Apple/Google, PACT,...]</th>
<th>Epione [TSS+20]</th>
<th>CleverParrot [CKL+20]</th>
<th>This Work [mSense/PSI-WCA]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Servers</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Server</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Number of Servers</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td><strong>Privacy</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Graph</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User-to-user</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Robustness Against</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relay</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replay</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upload Omission</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Feature</td>
</tr>
<tr>
<td>Trace Omission</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Centralized [TraceTogether,...]</td>
<td>Decentralized [D3-PT, Apple/Google, PACT,...]</td>
<td>Epione [TSS+20]</td>
<td>CleverParrot [CKL+20]</td>
<td>This Work [mSense/ PSI-WCA]</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------</td>
<td>------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td><strong>Tracing Cost</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User to Server Comm</td>
<td>O(n)</td>
<td>N/A</td>
<td>O(n log N)</td>
<td>N/A</td>
<td>O(nk)</td>
</tr>
<tr>
<td>Server to User Comm</td>
<td>O(1)</td>
<td>O(N)</td>
<td>O(n)</td>
<td>O(N')</td>
<td>O(1)</td>
</tr>
<tr>
<td>User Crypto Work</td>
<td>N/A</td>
<td>Non-crypto O(N) match</td>
<td>O(n) asym</td>
<td>O(N') asym</td>
<td>O(n) sym</td>
</tr>
<tr>
<td>Server Crypto Work</td>
<td>Non-crypto match</td>
<td>N/A</td>
<td>O(nN) asym</td>
<td>N/A</td>
<td>O(N) sym</td>
</tr>
<tr>
<td><strong>Rounds</strong></td>
<td>1</td>
<td>0.5</td>
<td>2</td>
<td>0.5</td>
<td>1</td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>Yes/No</td>
<td>All &quot;infected tokens&quot;</td>
<td>Count of exposures</td>
<td>Tokens of exposures</td>
<td>Weighted risk score</td>
</tr>
<tr>
<td>Result Returned</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Underlying Crypto</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Crypto Tools</td>
<td>Central trust</td>
<td>PRF-style &quot;PSI&quot;</td>
<td>DH-style PSI-CA plus 2PIR</td>
<td>DH-style PSI</td>
<td>PSI-(W)CA from FSS</td>
</tr>
</tbody>
</table>
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!
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)

$$P(x) = \begin{cases} b & \text{if } x=a \\ 0 & \text{otherwise} \end{cases}$$
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
Stealth Software Technologies, Inc.

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

Diagram:

- Google/Apple APIs
- Application Processor
- Low Power Sensors Subsystem
- Client API
- Sensors Execution Environment (SEE)
- Sensor API
- Sensor Drivers
- Algorithms

Legend:
- QC components
- API components
- 3rd Party components

Kryptowire Trusted App(s)
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 $P_i$:

\[
\text{response}_b = \sum_{i=1}^{n} \sum_{j=1}^{N} P_{i,b}(y_j)
\]

Sum of the responses = weighted risk score!

• Naïve computation is $O(nN)$, we also use careful combinatorial hashing to reduce server work
Reveal all infected tokens (Apple/Google, D3-PT)
+ Client can analyze matched tokens
- Leaks matches
- No token context

Reveal count of infected tokens encountered (Epione)
+ Hides token match while providing count
- Counts alone gives no context or risk data

Reveal sum of context-aware weights (Kryptowire + Stealth)
+ Hides token match while providing count
- Counts alone gives no context or risk data

"Trusted"
Reveal yes/no
+ Hides everything
- Yes/no alone not useful in metropolitan areas

Privacy

Utility

- 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
Thank You!

Paper