Digital Contact Tracing: Interoperability, Privacy and Scalability

Yaling Yang (Virginia Tech)

Patrick Schaumont (Worcester Polytechnic Institute)

Xiang Cheng (VT), Hanchao Yang (VT), Archanaa S Krishnan (WPI)

1/21/2021

Contact Tracing

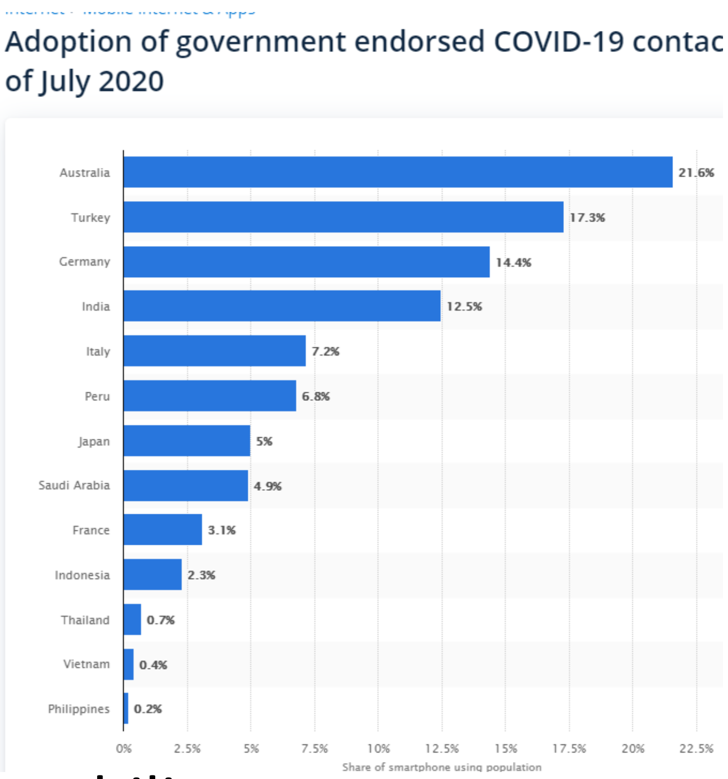
- Contact tracing: process of identifying people that may have come into contact with an infected person
- Help manage infectious diseases (such as Covid 19 pandemic) by quickly identifying new cases before they can infect others
- If speed of identifying new cases is close to speed of disease spreading, it can help to curb the spread of the disease

Type of Contact Tracing

- Manual Contact Tracing;
  - Human workers interview with patients to find their contacts and visited locations in the past
  - Labor intensive and expensive
    - In US, analysts estimate that effective manual contact tracing would require 100k-300k workers and $3 billion-$12 billon in spending
  - May not identify contacts that are strangers
- Digital Contact Tracing (DCT)
  - Automate the collection of contact data using smartphone apps
  - Can identify contacts that do not know each other
  - Can potentially perform tracing more quickly, cheaper and at a larger scale

DCT Challenges

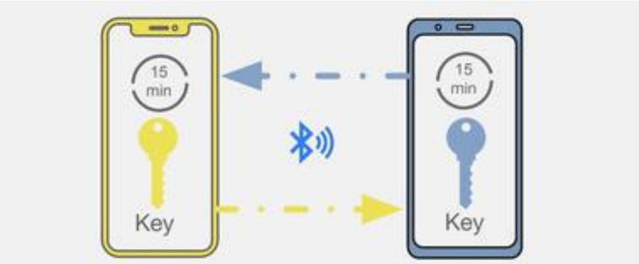
- Privacy
  - User identity, user location trajectory, user social contacts are all sensitive personal data
  - Needs protection
- Adoption rate
  - Public distrust in operators of DCT systems hinders adoption
  - Ownership of mobile phones are low in some very vulnerable demographics (e.g. seniors, or residents in developed countries)
- Scalability
  - Needs to scale to support large number of users


Adoption of government endorsed COVID-19 contac
of July 2020

- Interoperability
  - Can DCT provide useful information to manual contact tracing?
  - Can DCT provide useful aggregated information to health authority?
- Accuracy

Bluetooth DCT

- Mechanism
  - Phone exchange anonymous random IDs



  - If a smartphone owner tests positive, the app uploads transmitted random IDs to server
  - Other devices retrieve patients' IDS from the server and compare them with received IDs to find past encounters with patients

- Problem
  - Both phones have to have the app to work
    - Must have high adoption rate
  - Cannot interoperate with manual contact tracing
    - Cannot provide useful information to manual contact tracing
    - Cannot benefit from manual contact tracing
  - Can only capture direct face-to-face spreading
    - How about indirect spreading? E.g. contaminated surface to person? Airborne aerosol spreading?

Our Argument: Geolocation DCT

- Mechanism
  - Phones log location trajectories using GNSS technology (e.g. GPS)
  - Trajectories are compared to identify intersections
  - If a smartphone owner tests positive, the app can send an alert to devices that have trajectory intersections with the patient.
- Benefit: Interoperability with manual contact tracing
  - Information exchanged between DCT and manual contact tracing
    - Locations where patients have visited
  - Ensure phone-less demographics can also benefit from DCT system

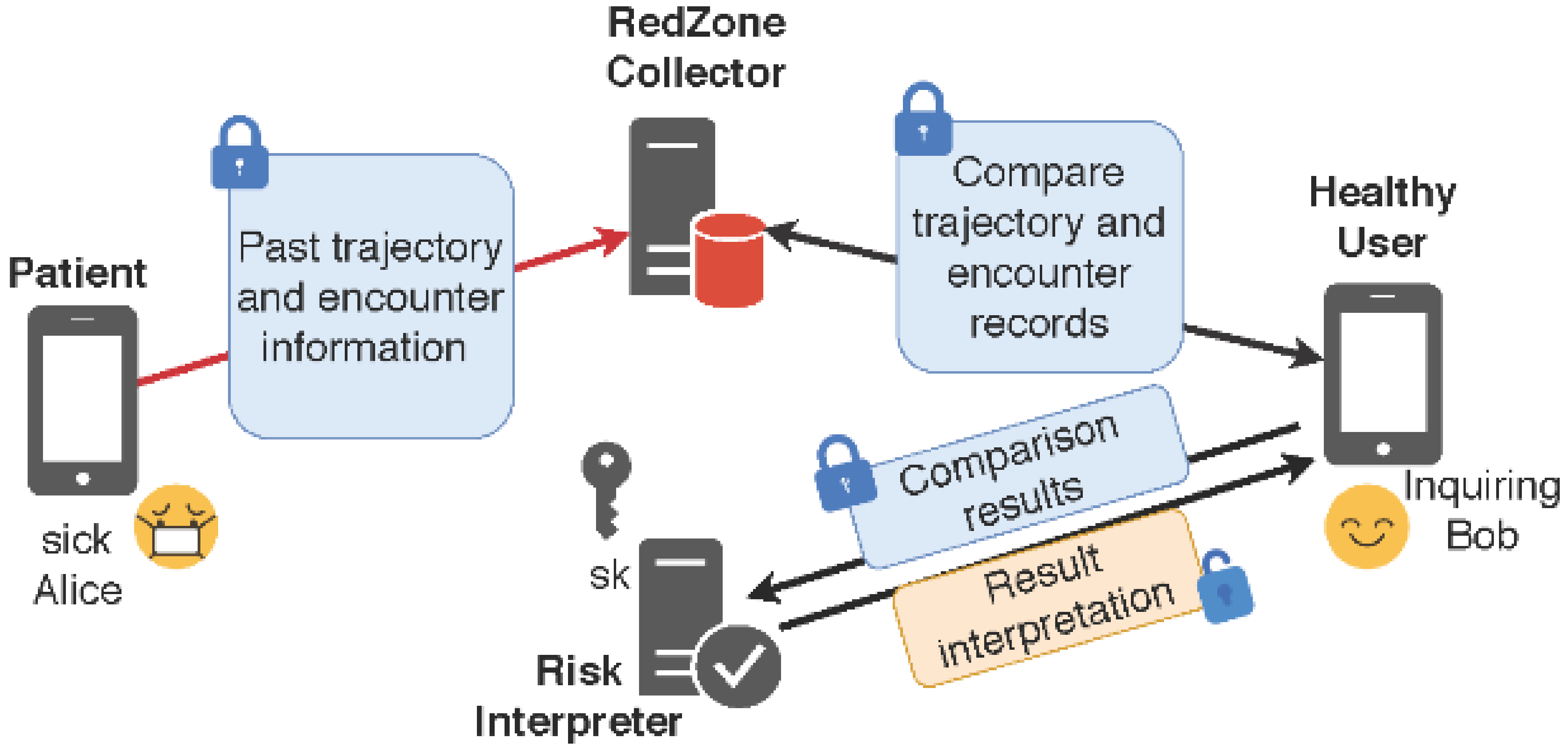
Challenges to Geolocation DCT

- How to protect location privacy of users from untrusted servers, other users, and general public?
- Indoor?

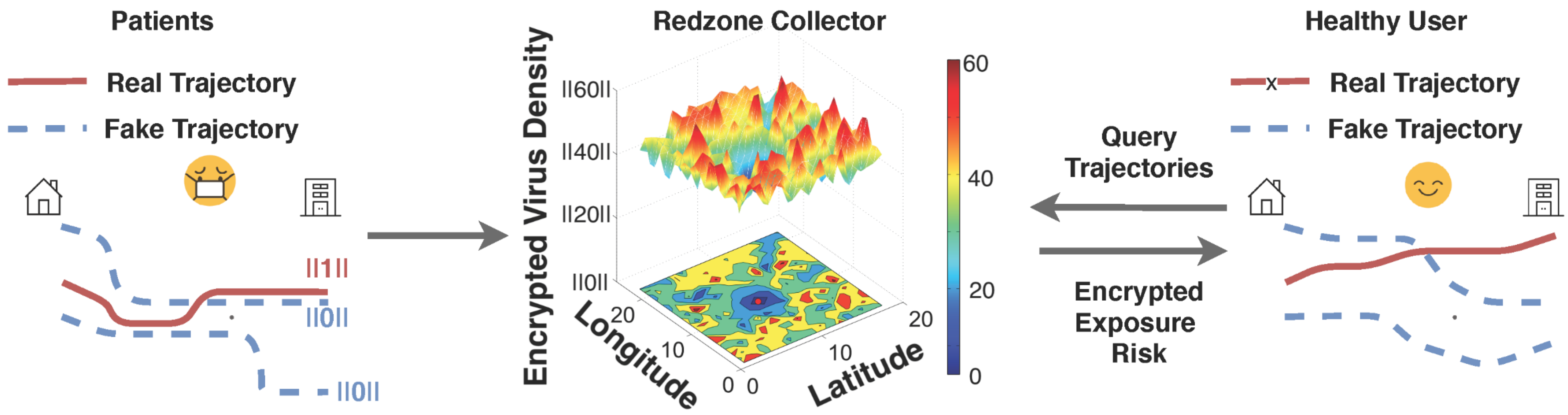
Our work: Interoperable Privacy-Preserving DCT

- A novel DCT named **KHOVID** that
  - Combine geolocation with Bluetooth → accurate in all environments
  - Provide privacy protection to both patients and healthy users against untrusted servers, other users and general public
    - K-anonymity
    - Secure multiparty computation
  - Provide mechanism to capture both direct and indirect spreading

KHOVID overview



Geolocation contact tracing in KHOVID

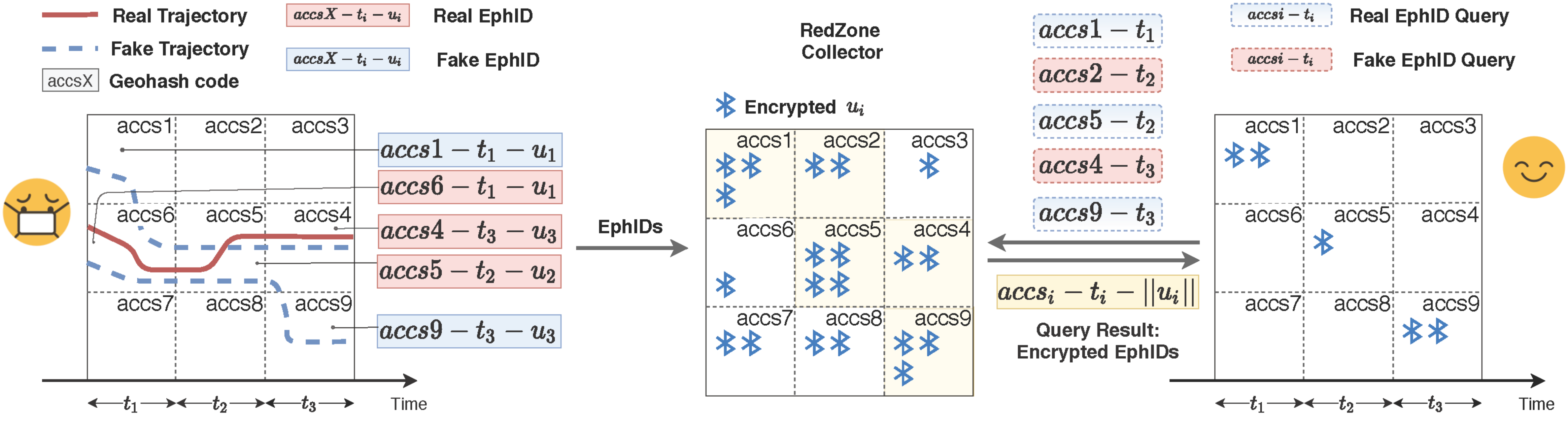


- Mixing real and fake trajectories
- Homomorphic encrypted flag to mark (0/1 =fake/real)
  - Can be extended to represent potential amount of virus shedding

- Homomorphic aggregation of patient inputs → Encrypted virus density map
- Retrieve and homomorphically aggregate virus load for each received query trajectories → risk level

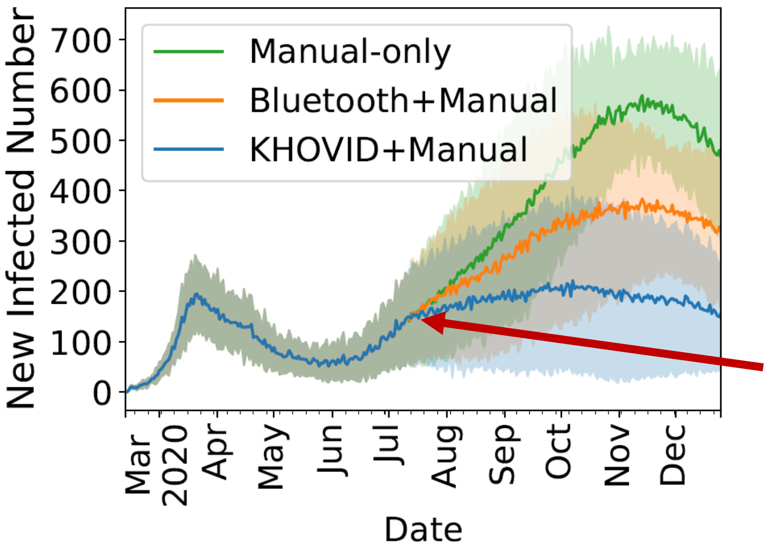
- Mixing real and fake trajectories
- Receive risk levels for each query trajectory and pick the one corresponding to the real trajectory

Bluetooth contact tracing in KHOVID

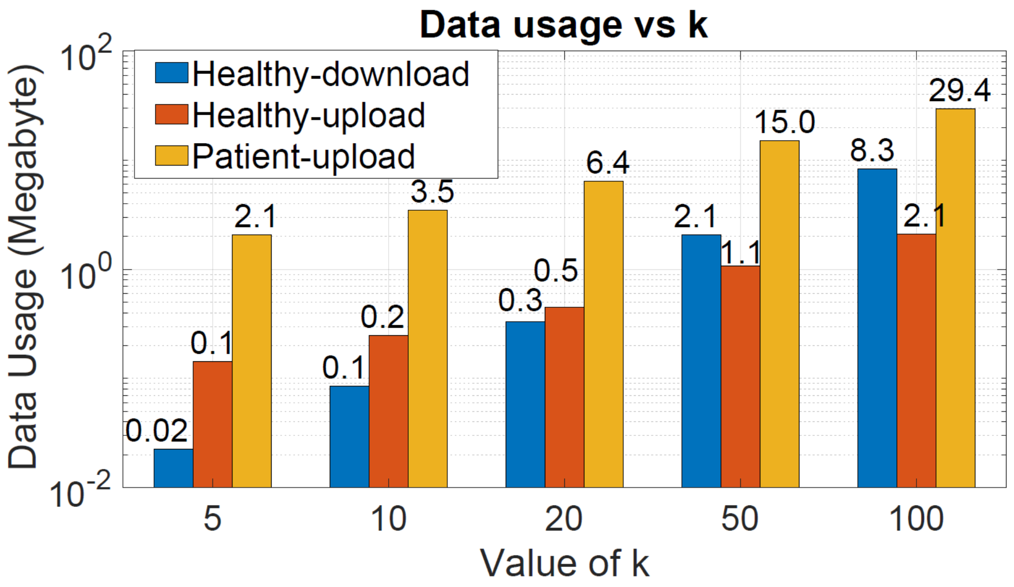


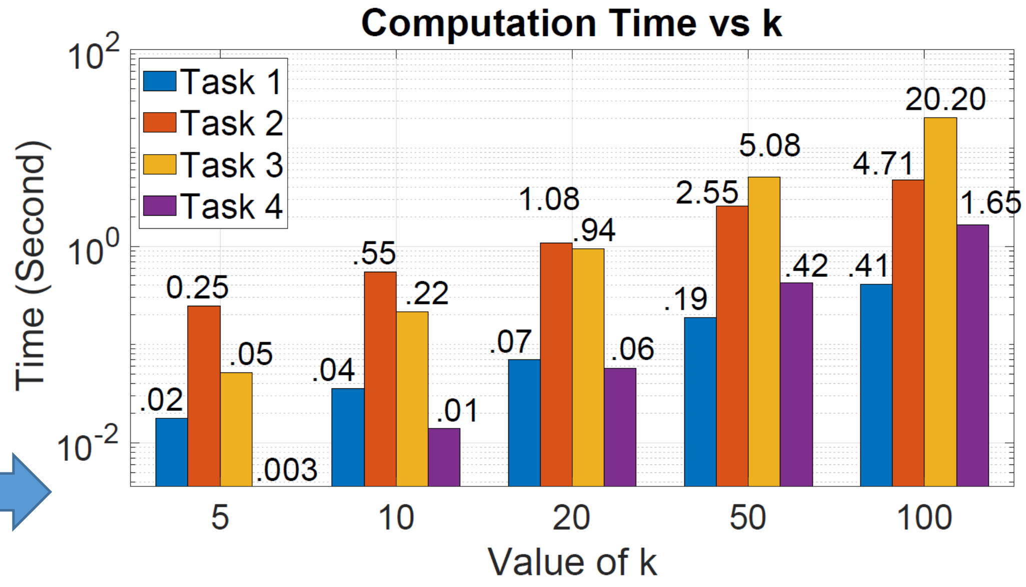
Performance of KHOVID

Daily new cases when DCT has 30% adoption rate


Snohomish County

DCT is deployed





Computation time of (1) processing query result, (2) encrypting patient's data before upload, (3) integrating patient data input and (4) computing exposure risk for a user query.

Summary

- In public health crisis, DCT has to balance many considerations
  - Privacy
  - Scalability
  - Interoperability
  - Flexibility
- Our KHOVID DCT design is an effort in this direction