The Rise (and Fall?) of (De)Centralized Automatic Contact Tracing

Gennaro Avitabile, Vincenzo Botta, Vincenzo Iovino, Ivan Visconti

(DIEM - University of Salerno)

How to Notify Risks of Infection?

Matthew Green on March 19: (more or less)

just use rotating pseudonyms as identifier beacons using Bluetooth-Low-Energy, like in Apple's "Find my" system... the solution is already there

IDs of infected citizens can then be sent to a server that sends them back to everyone interested in checking recent proximity to them

How to Notify Risks of Infection?

Matthew Green on March 19: (more or less)

just use rotating pseudonyms as identifier beacons using Bluetooth-Low-Energy, like in Apple's "Find my" system... the solution is already there
IDs of infected citizens can then be sent to a server that sends them back to everyone interested in checking recent proximity to them

it is simple, efficient, seemingly decentralized/privacy preserving

How to Notify Risks of Infection?

Matthew Green on March 19: (more or less)

just use rotating pseudonyms as identifier beacons using Bluetooth-Low-Energy, like in Apple's "Find my" system... the solution is already there
IDs of infected citizens can then be sent to a server that sends them back to everyone interested in checking recent proximity to them

it is simple, efficient, seemingly decentralized/privacy preserving

…then…. DP-3T, PACT-... and Apple-Google APIs....
…the rise of so called "decentralized contact tracing"...

How to Notify Risks of Infection?

Matthew Green on March 19: (more or less)

just use rotating pseudonyms as identifier beacons using Bluetooth-Low-Energy, like in Apple's "Find my" system... the solution is already there
IDs of infected citizens can then be sent to a server that sends them back to everyone interested in checking recent proximity to them

it is simple, efficient, seemingly decentralized/privacy preserving

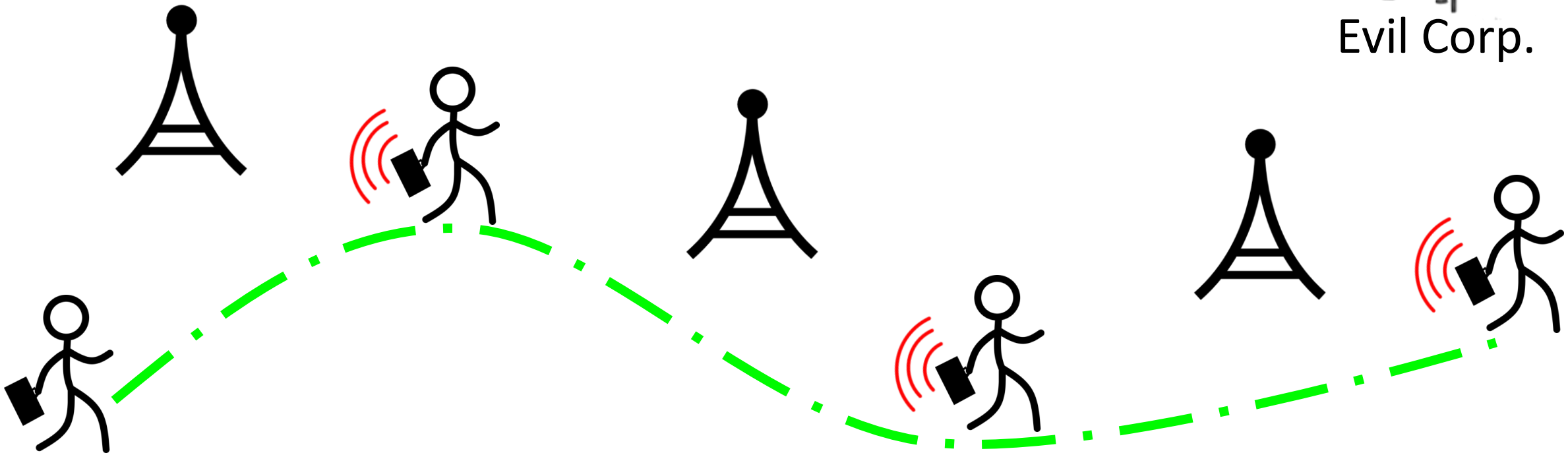
…then…. DP-3T, PACT-... and Apple-Google APIs....
…the rise of so called "decentralized contact tracing"...

severe criticism against PEPP-PT and ROBERT that proposed a centralized version where pseudonyms are generated by the server

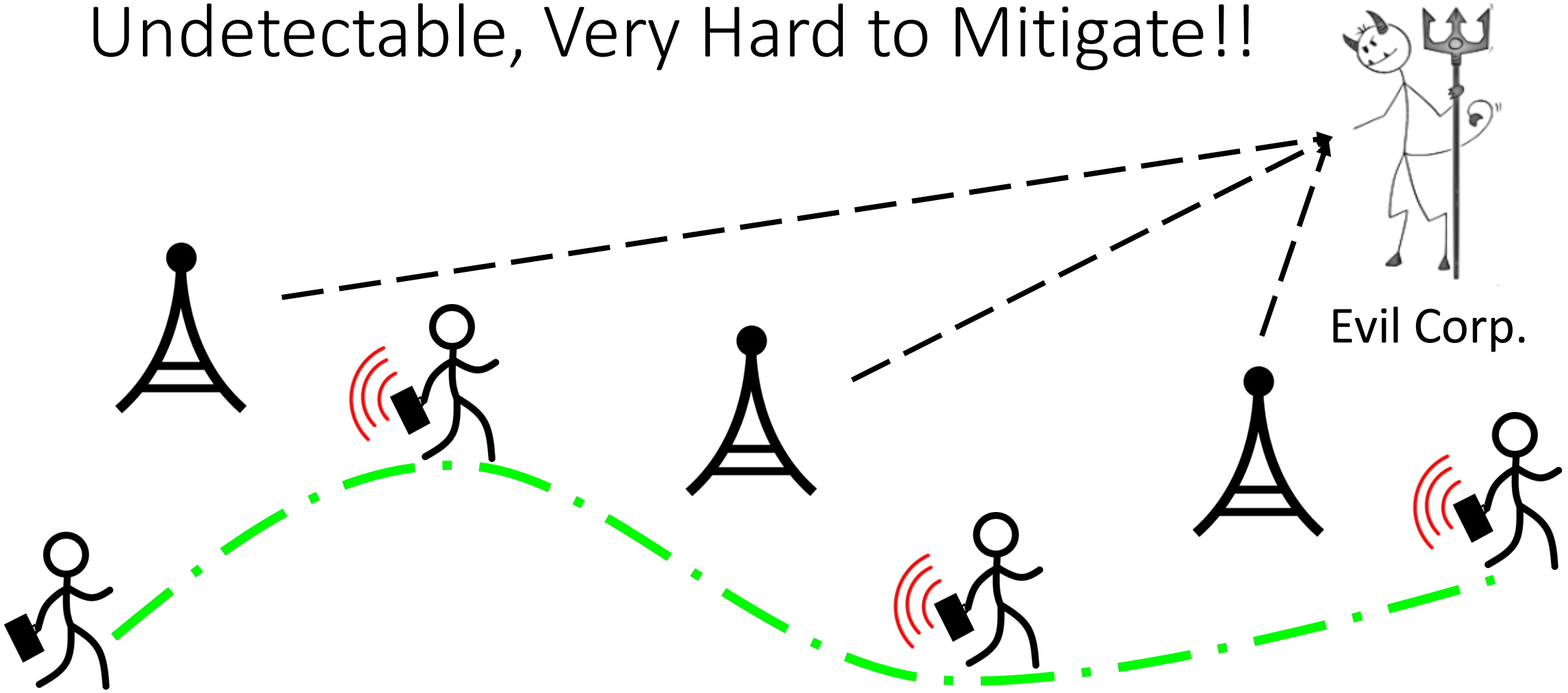
Serge Vaudenay: Paparazzi Attack!

https://eprint.iacr.org/2020/399

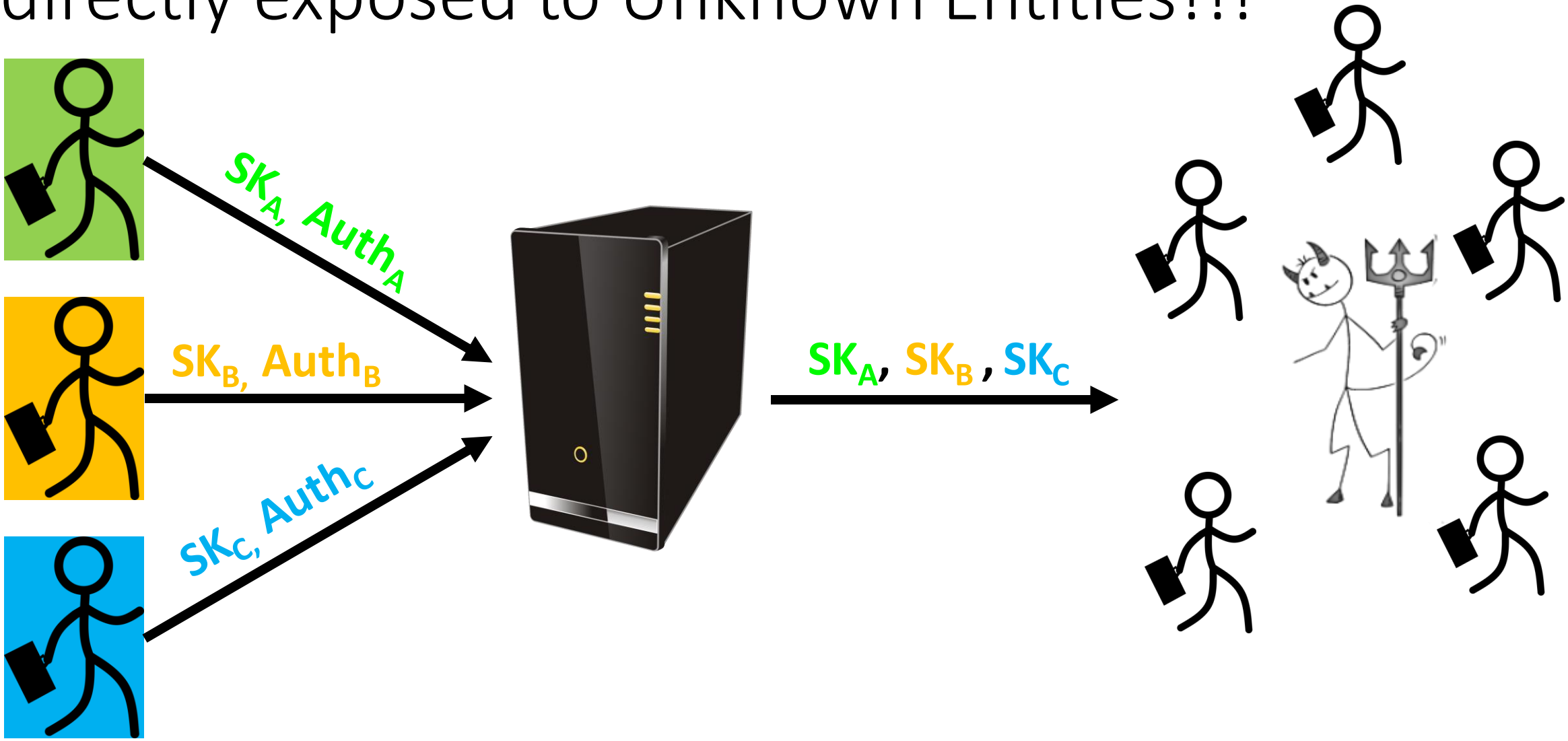
Evil Corp.



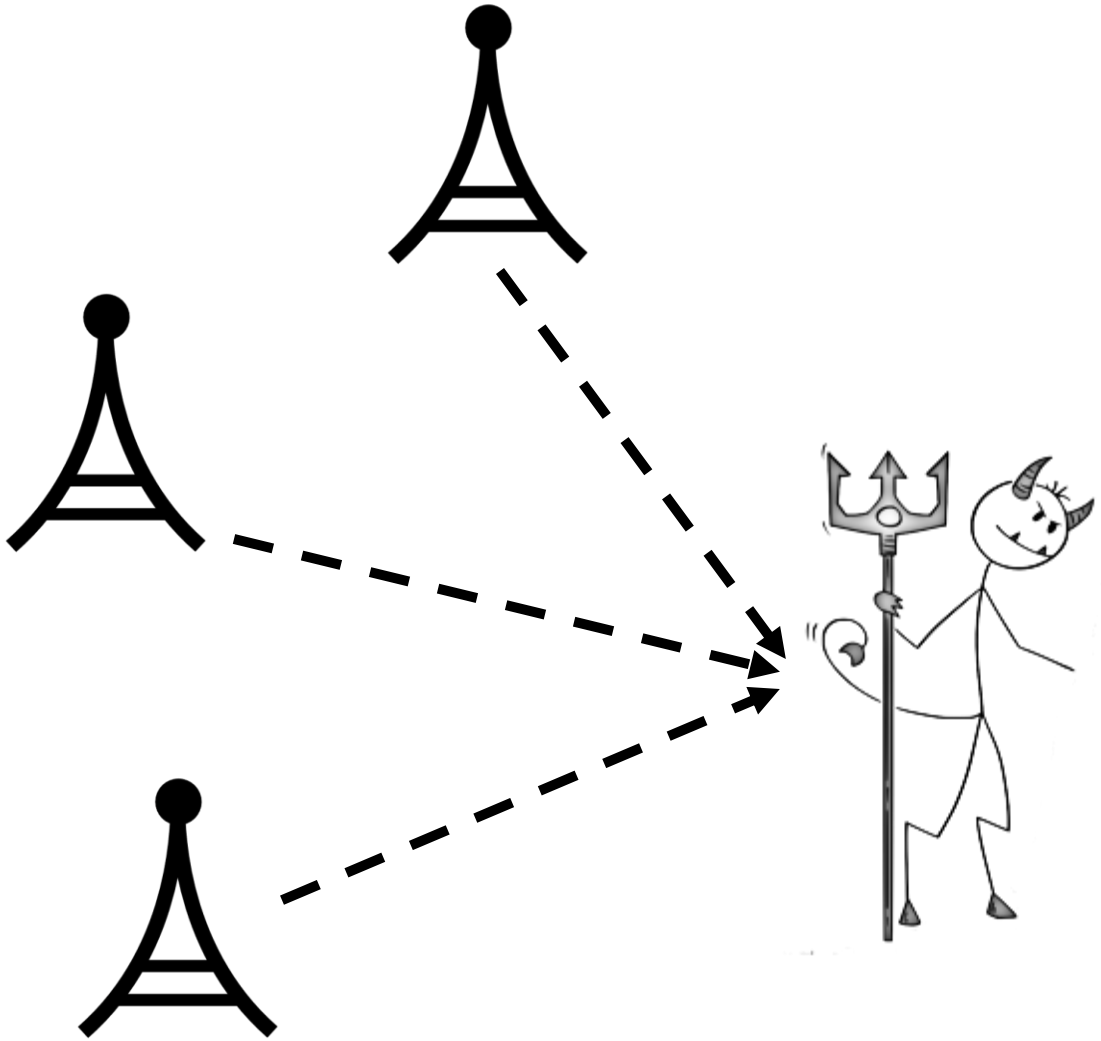
Paparazzi Attack: Passive and Undetectable, Very Hard to Mitigate!!



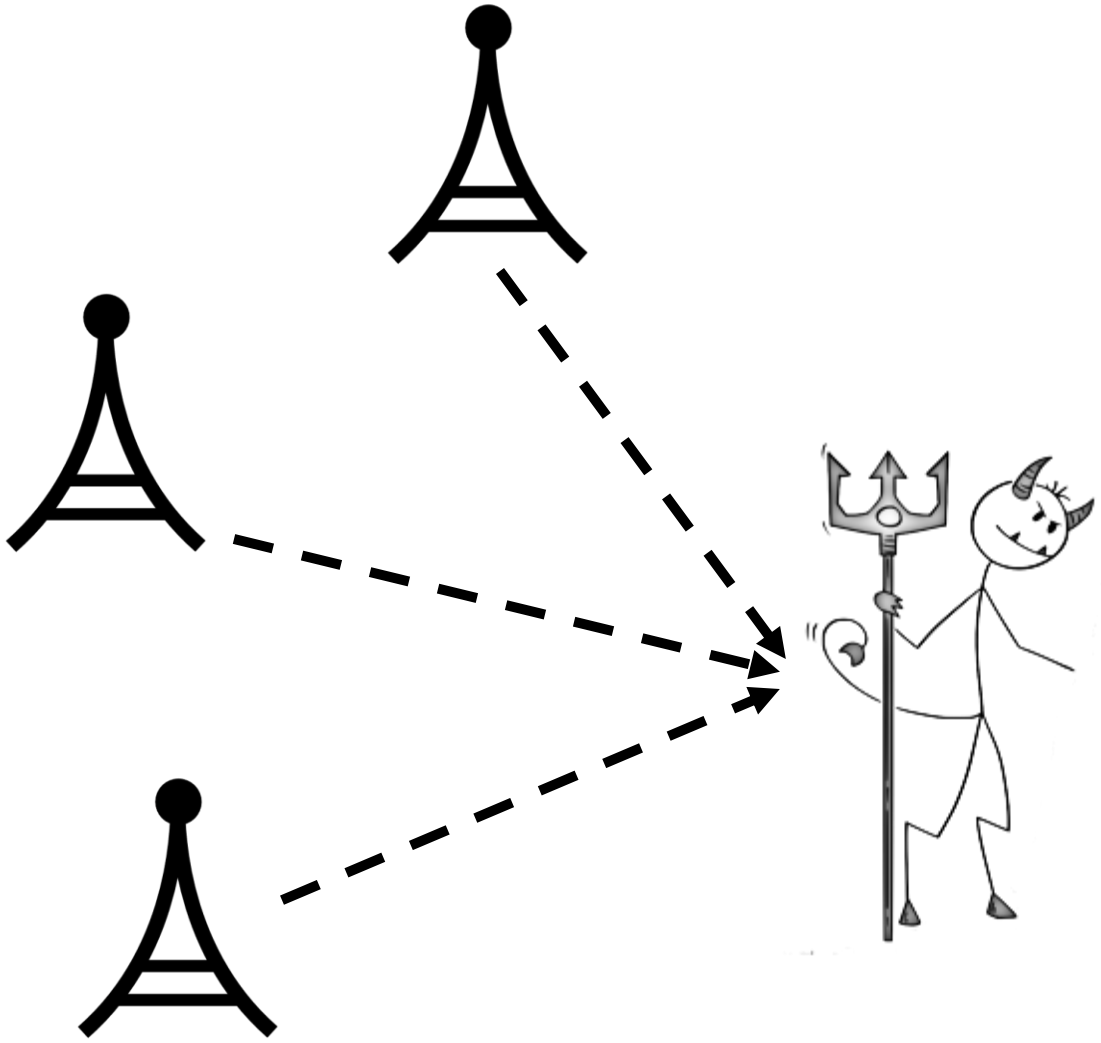
Paparazzi Attack: Private data of Citizens directly exposed to Unknown Entities!!!

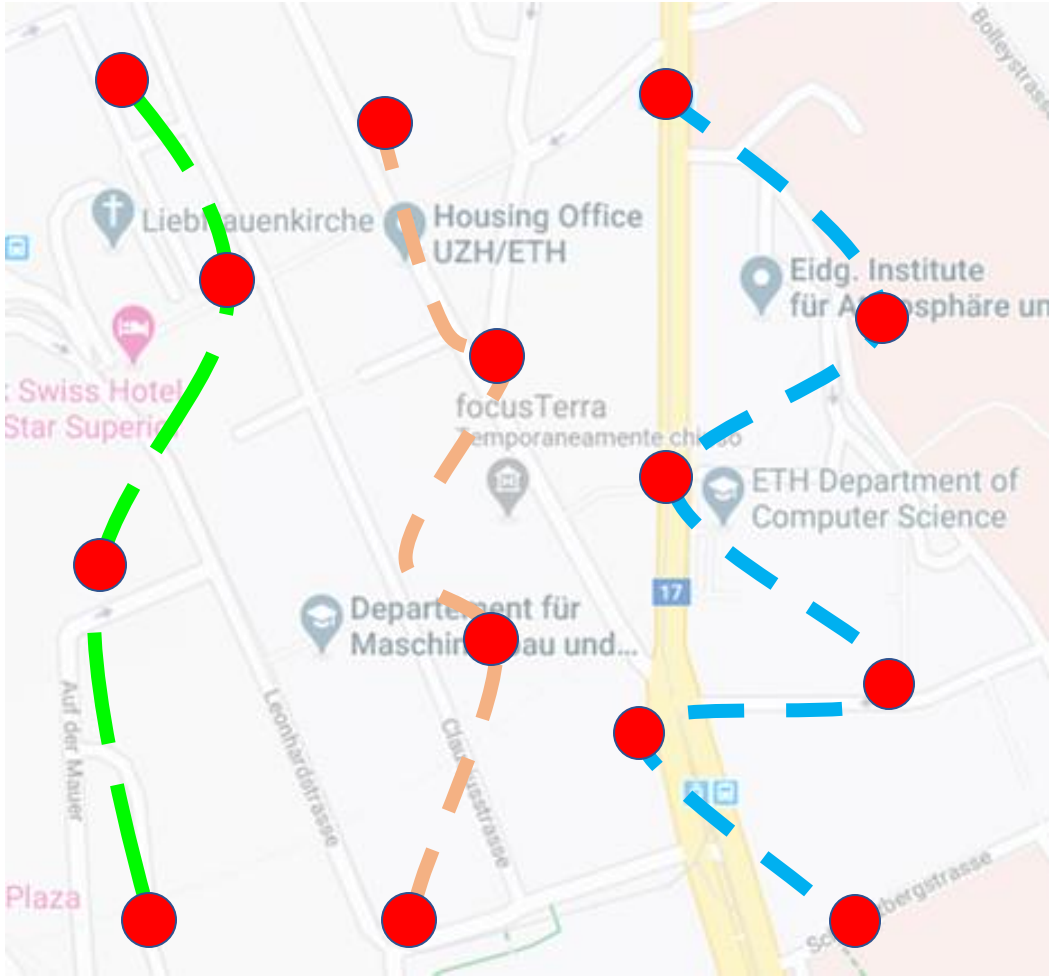


and then….



Mass Surveillance!!!! This is very scary!!!!!





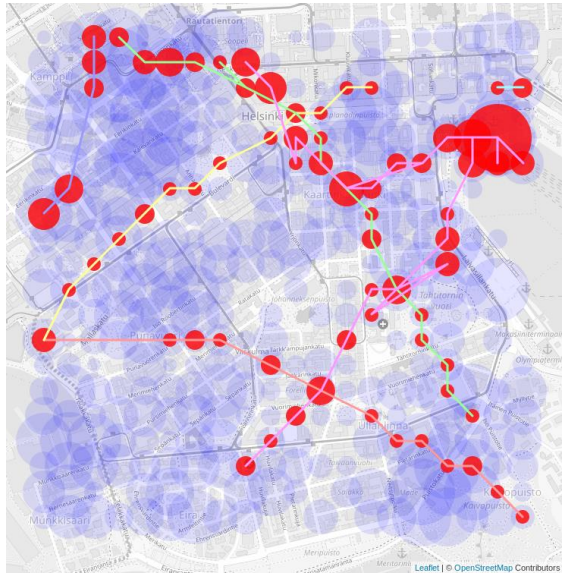
SK_A SK_B SK_C

Paparazzi Attack - Mass Surveillance

- DP-3T low-cost design is affected by this attack
  https://github.com/DP-3T/documents

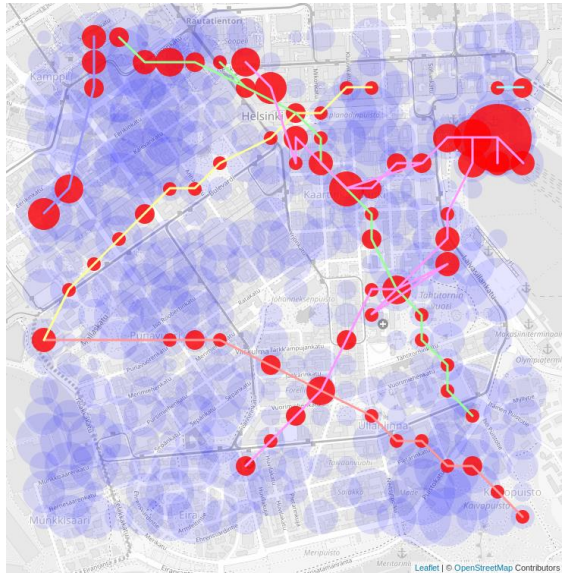
Paparazzi Attack - Mass Surveillance

- DP-3T low-cost design is affected by this attack
  https://github.com/DP-3T/documents
- Otto Seiskari showed a PoC implementation of the attack to DP-3T https://github.com/oseiskar/corona-sniffer



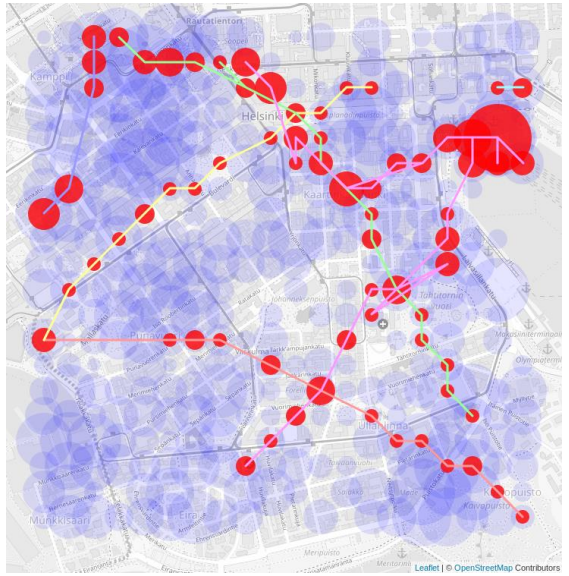
Paparazzi Attack - Mass Surveillance

- DP-3T low-cost design is affected by this attack
  https://github.com/DP-3T/documents
- Otto Seiskari showed a PoC implementation of the attack to DP-3T https://github.com/oseiskar/corona-sniffer
- Surprise: ROBERT instead withstands this attack
  https://github.com/ROBERT-proximity-tracing/documents

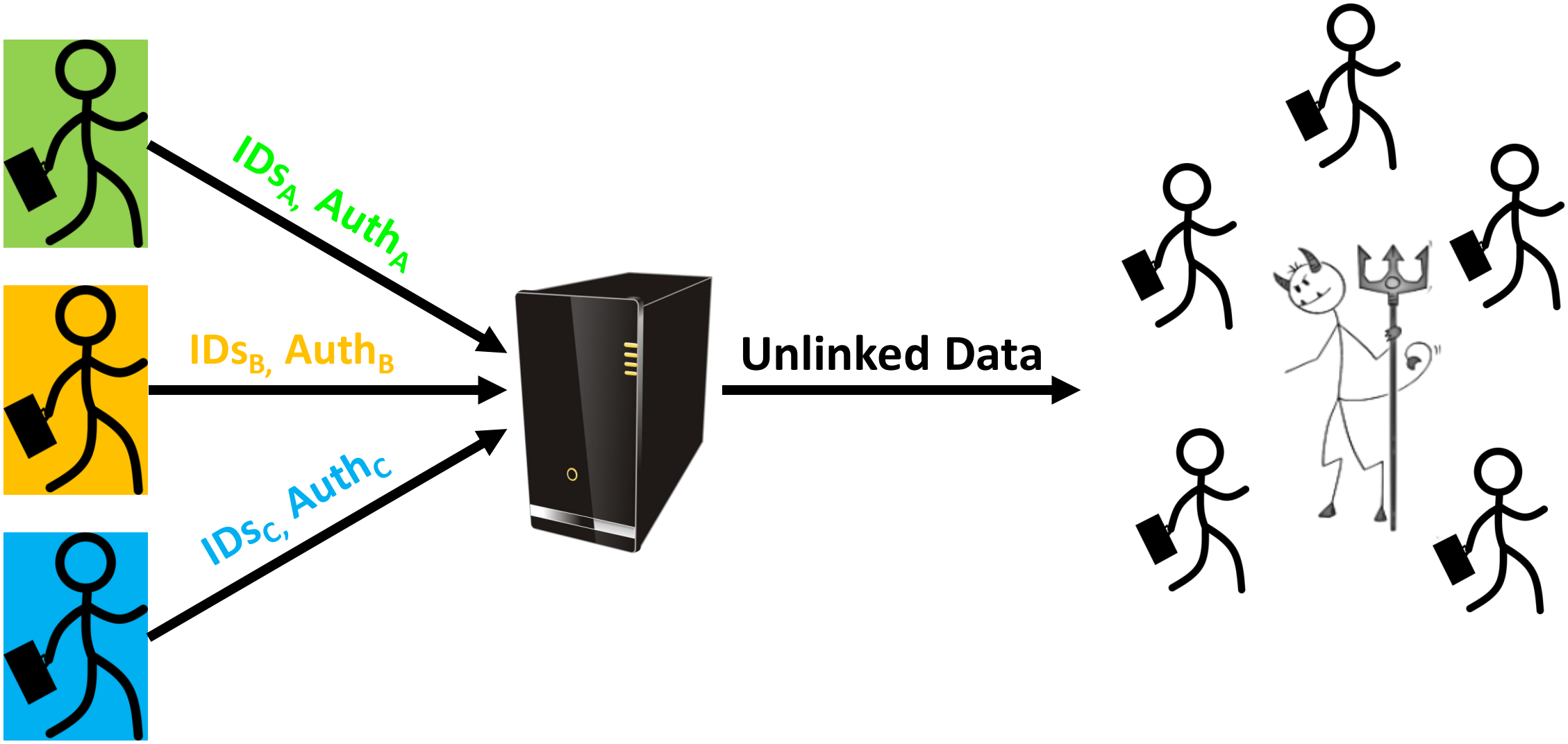


Paparazzi Attack - Mass Surveillance

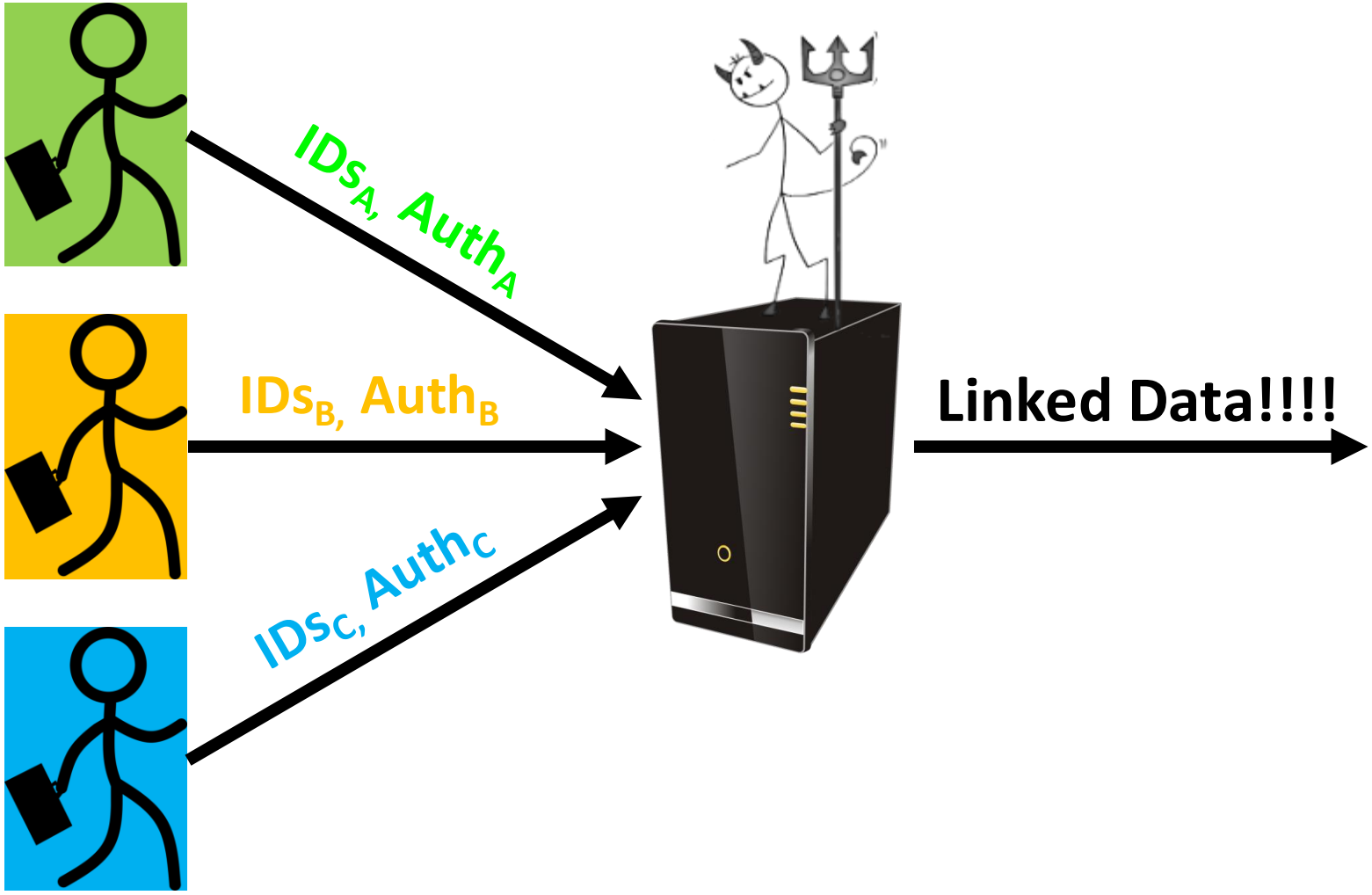
- DP-3T low-cost design is affected by this attack
  https://github.com/DP-3T/documents
- Otto Seiskari showed a PoC implementation of the attack to DP-3T https://github.com/oseiskar/corona-sniffer
- Surprise: ROBERT instead withstands this attack
  https://github.com/ROBERT-proximity-tracing/documents
- DP-3T unlinkable design withstands this attack... but...



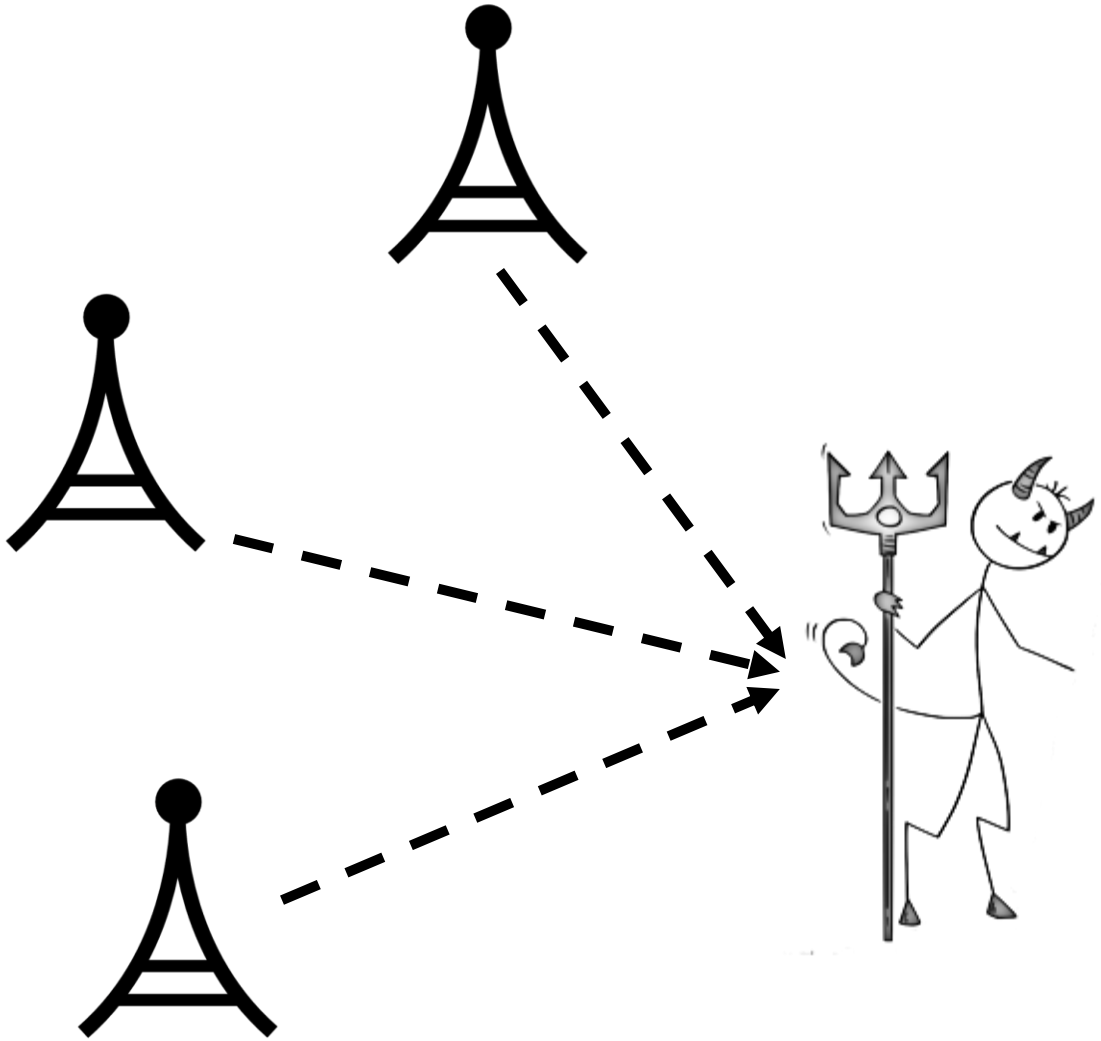
DP-3T Unlinkable Design

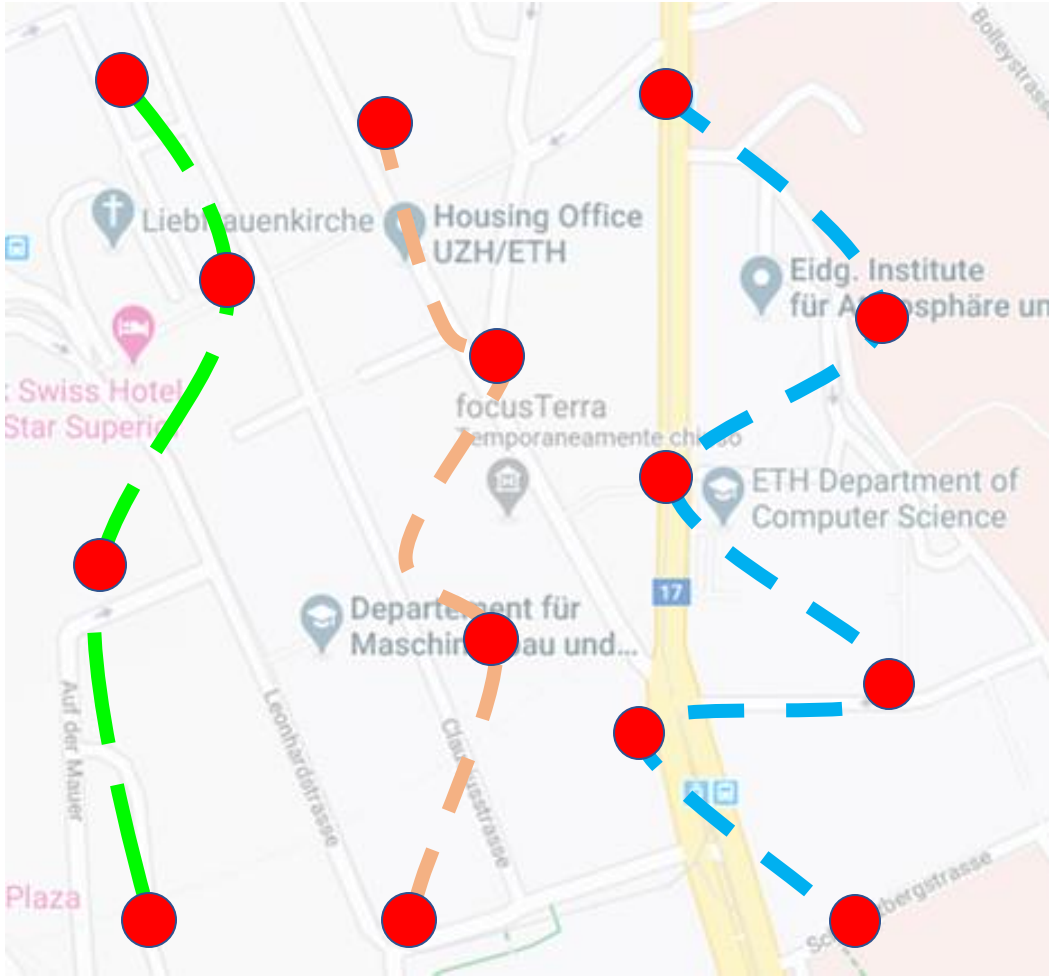


Orwell Attack - Mass Surveillance!!!!



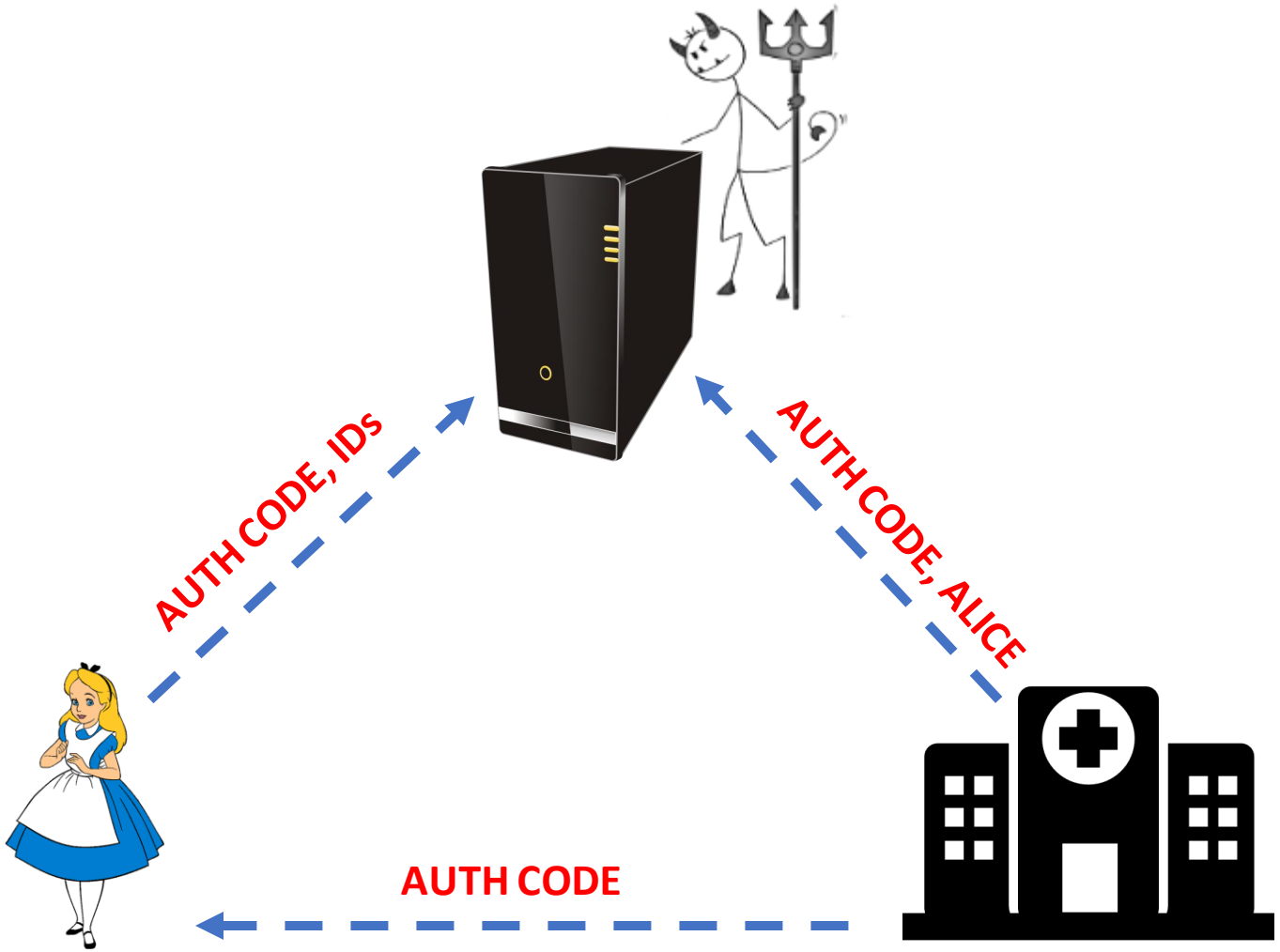
Orwell Attack - Mass Surveillance – Passive BLE receivers – Hard to Mitigate!!!!!



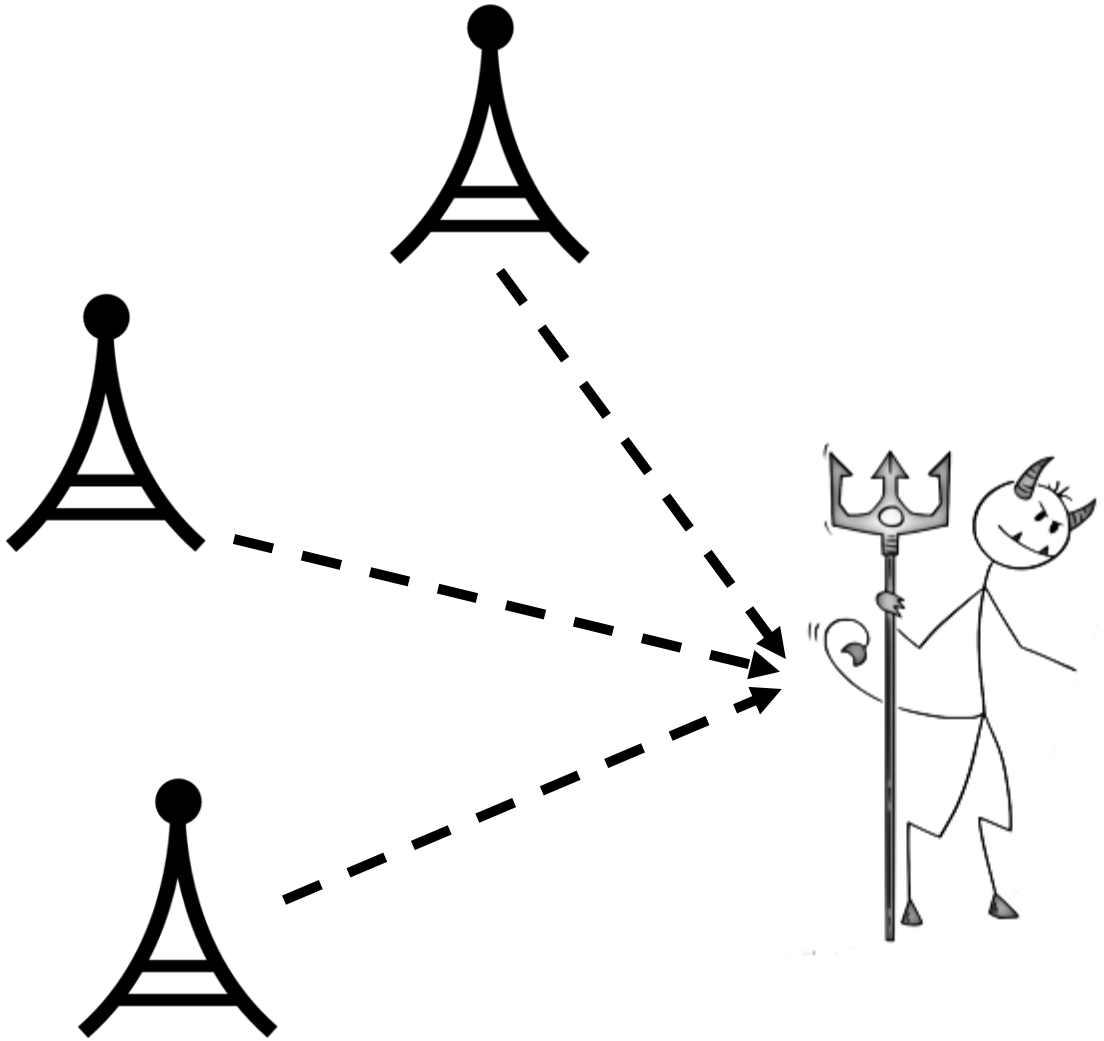


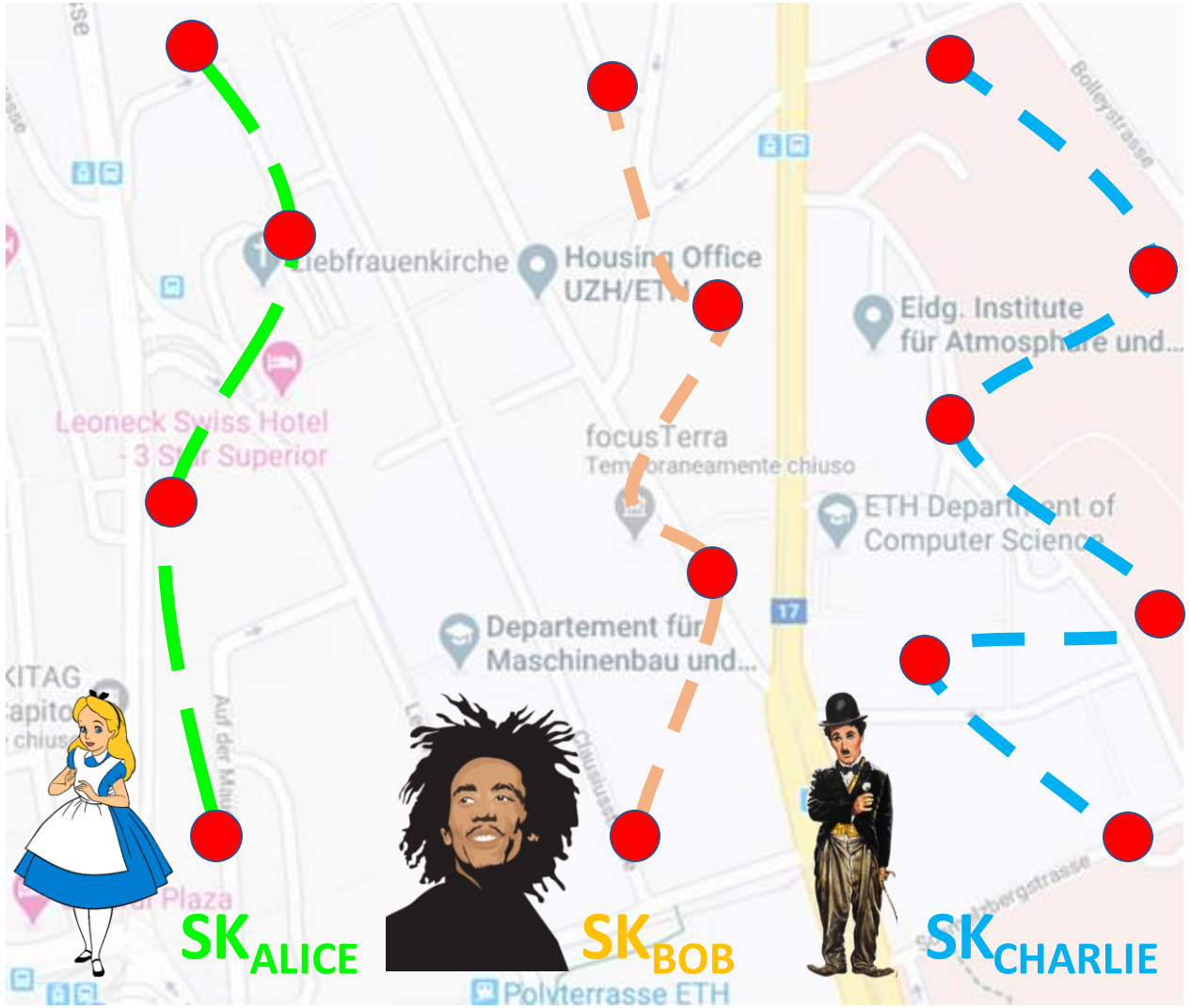
SK_A SK_B SK_C

Brutus Attack - Mass Surveillance



Brutus Attack + Orwell Attack!!!!!!





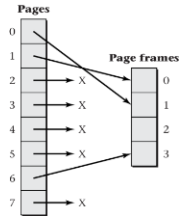
Contact Tracing: Decentralization? Privacy?

- DP-3T: Low-cost design: decentralized, but with serious privacy issues w.r.t. hard-to-mitigate attacks (i.e., Paparazzi, Orwell, Brutus attacks)
- DP-3T: Unlinkable design: semi-centralized, with serious privacy issues w.r.t. hard-to-mitigate government attacks (i.e., Orwell, Brutus attacks)
- Robert: centralized, with very serious privacy issues w.r.t. government attacks (i.e., Orwell Attack)
- Serge Vaudenay: "We should look for a third way"
  https://eprint.iacr.org/2020/531

Pronto-C2 (https://eprint.iacr.org/2020/493)

Anonymous Calls

70's Crypto



Pointers

Features	Pronto-C2	Low-cost DP-3T Endorsed by A&G	Unlinkable DP-3T
Resilience to Paparazzi Atk	✓	✗	✓
Resilience to Orwell Atk	✓	✗	✗
Resilience to Brutus Atk	✓	✗	✗
Decentralized	✓	✓	✗

Edward Snowden, about 5 weeks ago

- ***Do you truly believe that*** *when the first wave, the second wave, the 16th wave of the coronavirus is a long-forgotten memory, that these capabilities will not be kept, that* ***these data sets will not be kept?*** *Will those capabilities begin to be applied to small-time criminality? Will they begin to be applied to political analysis? Will they begin to be applied for doing things like performing a census? Will they be used for political polling?* ***No matter how it is being used, what is being built is the architecture of oppression.*** *And* ***you might trust who is dealing with it****, you might trust who runs it. You might go, "You know, I don't care about Mark Zuckerberg."* ***But someone else will have this data eventually****. Some other country will have this data eventually. In your country, a different president will have control of this data eventually,* ***and someone will abuse it****.*
- https://www.youtube.com/watch?v=k5OAjnveyJo

Thanks a lot for your attention! Work done with our very limited but valuable resources…. our time.