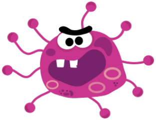
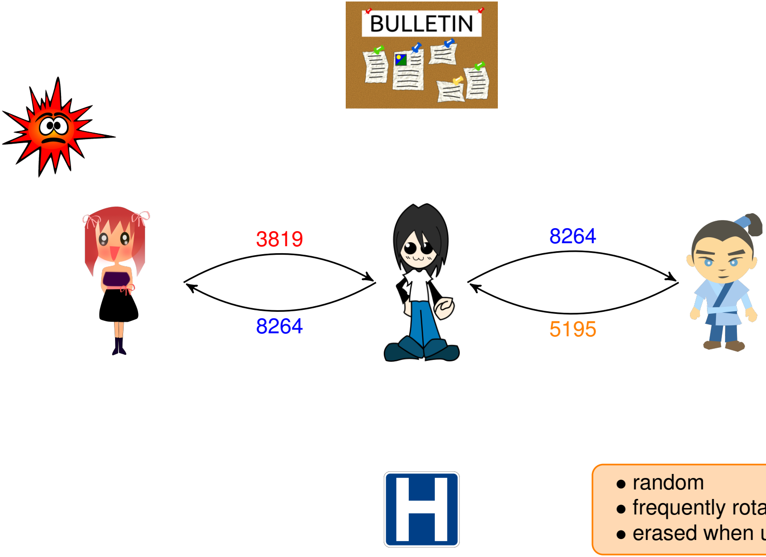
Chasing Infected People

Serge Vaudenay

EPFL

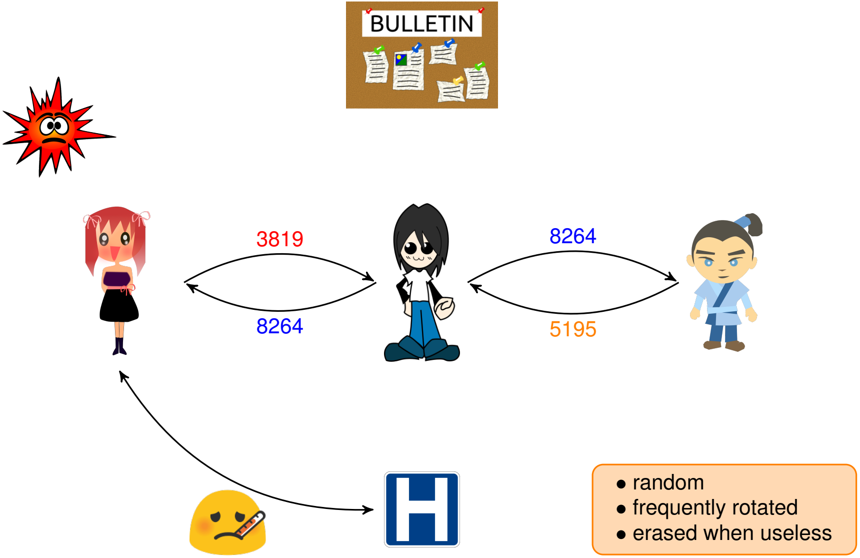


Decentralized Contact Tracing



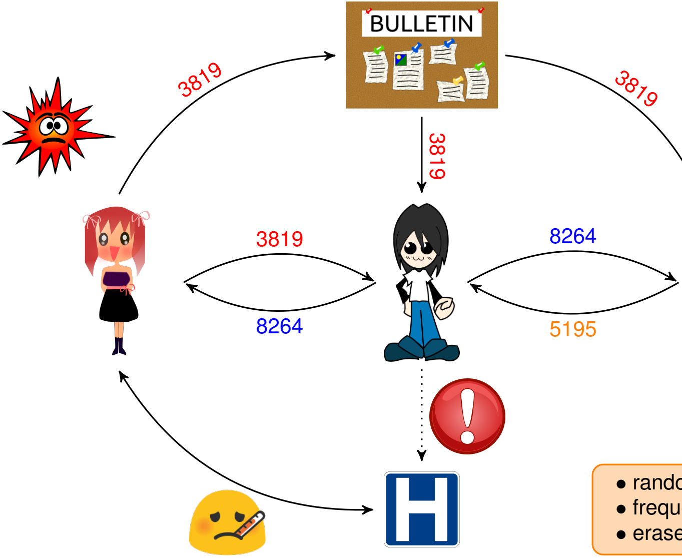
- random
- frequently rotated
- erased when useless

Decentralized Contact Tracing



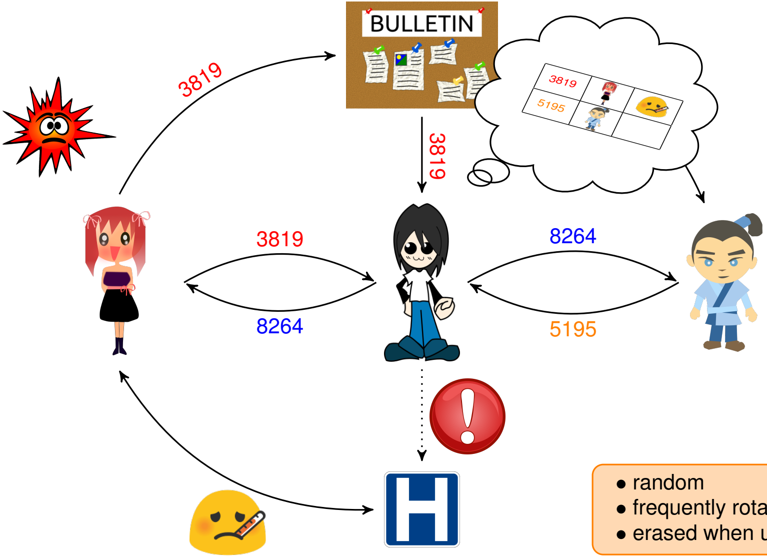
- random
- frequently rotated
- erased when useless

Decentralized Contact Tracing



- random
- frequently rotated
- erased when useless

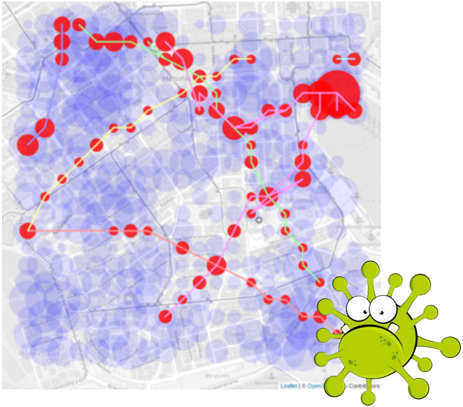
Decentralized Contact Tracing



- random
- frequently rotated
- erased when useless

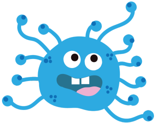
Deanonymization Attack of Diagnosed Reports

- wherever people identify: at hotel, company, shop
- paparazzi
- malicious app/OS/phone
- coupled with video-surveillance
- or even Bluetooth-only:



https://github.com/oseiskar/corona-sniffer

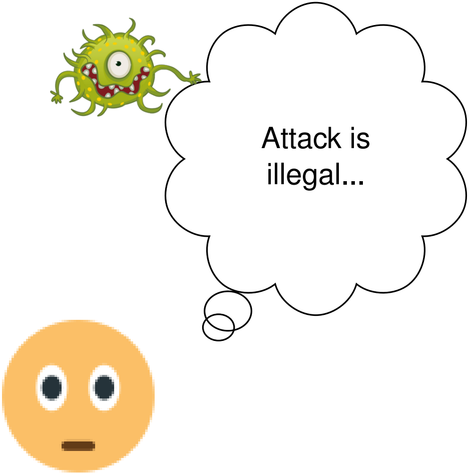
Countermeasure 1



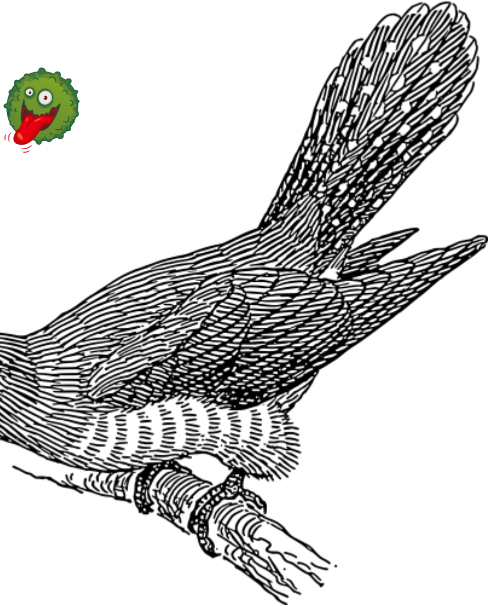
Countermeasure 2

Attack is too hard...

Countermeasure 3



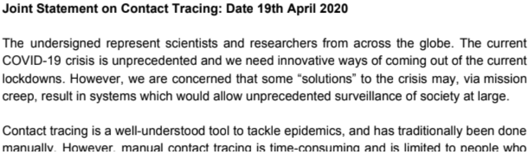
Countermeasure 4



Countermeasure 5

*

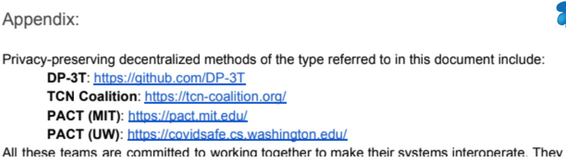
*



Joint Statement on Contact Tracing: Date 19th April 2020

The undersigned represent scientists and researchers from across the globe. The current COVID-19 crisis is unprecedented and we need innovative ways of coming out of the current lockdowns. However, we are concerned that some "solutions" to the crisis may, via mission creep, result in systems which would allow unprecedented surveillance of society at large.

Contact tracing is a well-understood tool to tackle epidemics, and has traditionally been done manually. However, manual contact tracing is time-consuming and is limited to people who



Appendix:

Privacy-preserving decentralized methods of the type referred to in this document include:

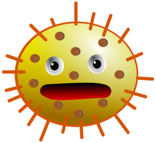
DP-3T: https://github.com/DP-3T
TCN Coalition: https://tcn-coalition.org/
PACT (MIT): https://pact.mit.edu/
PACT (UW): https://covidsafe.cs.washington.edu/

All these teams are committed to working together to make their systems interoperate. They

https://www.esat.kuleuven.be/cosic/sites/contact-tracing-joint-statement/

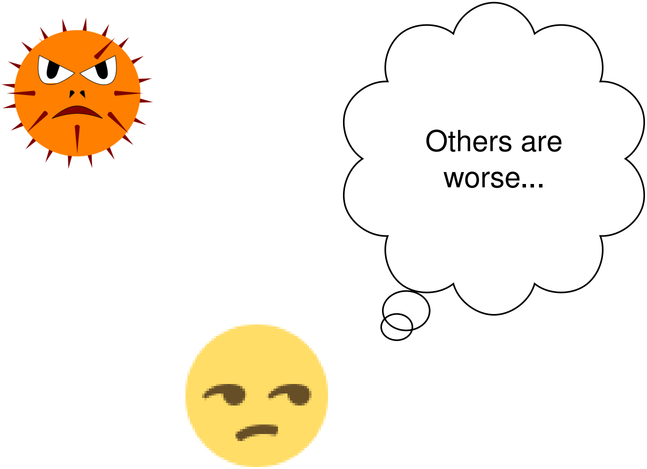
* Last minute edition + signature collection. Many other people contributed.

Countermeasure 6



It applies to
all
schemes...

Countermeasure 7



An Idea (Borrowed from Yuval)

Please don’t attack!

Why Not: Look for Alternatives?

- **Beskorovajnov et al.**: centralized + open server
- **Epione**: decentralized + private set intersection
- (Seen in **PACT-West**) report received *e*'s + rerandomize
- **Pronto-C2**: Diffie-Hellman + blockchain
- **DESIRE**: Diffie-Hellman + centralized

`https://eprint.iacr.org/2020/531`

Stay safe and healthy!

(You may be watched otherwise)