Anonymous communications
(a crash course in 7 minutes)

CPDP -
24th January 2018

Carmela Troncoso
carmela.troncoso@epfl.ch
Dear Dr. Bob,
Can we change my chemo appointment?
A.
But we can encrypt! What is the problem?

Destinyation: IP web
Dr. Bob Oncologist

A Network

Ethernet
(IEEE 802.3, 1997)

IPv4 Header
(RFC 791, 1981)

Same for TCP, SMTP, IRC, HTTP, ...
The problem is Traffic Analysis!!

A Network

Ethernet (IEEE 802.3, 1997)

IPv4 Header (RFC 791, 1981)

Same for TCP, SMTP, IRC, HTTP, ...

Weak identifier

Destination: IP web
Dr. Bob Oncologist
The solution: anonymous communications

- Bitwise unlinkability
  - Crypto to make inputs and outputs bit patterns different

- (re)packetizing + (re)schedule
  - Destroy patterns (traffic analysis resistance)
The solution: anonymous communications

- **Bitwise unlinkability**
  - Crypto to make inputs and outputs bit patterns different

- (re)packetizing + (re)schedule + (re)routing,
  - Destroy patterns (traffic analysis resistance)
  - Load balancing
  - Distribute trust
Anonymous communications out there

**LOW LATENCY**

Web browsing, Instant Messaging, streaming

**HIGH LATENCY**

Global Adversary resistance at the cost of latency (and long term patterns revealed)

Email, Voting

Cannot resist Global Adversary (assumes adversary cannot see both edges)

Bob is visiting CNN

Who exactly is Bob talking to?

**MIXMASTER / MIXMINION**

Panoramix

THE BEST OF BOTH WORLDS
Lots of challenges ahead!

Deploying new things or work on deployed ones
  – finding volunteers and diversity is a hassle

Modeling adversaries
  – we don’t know what the bad guys know

Measure anonymity
  – what is anonymity? when is it enough?