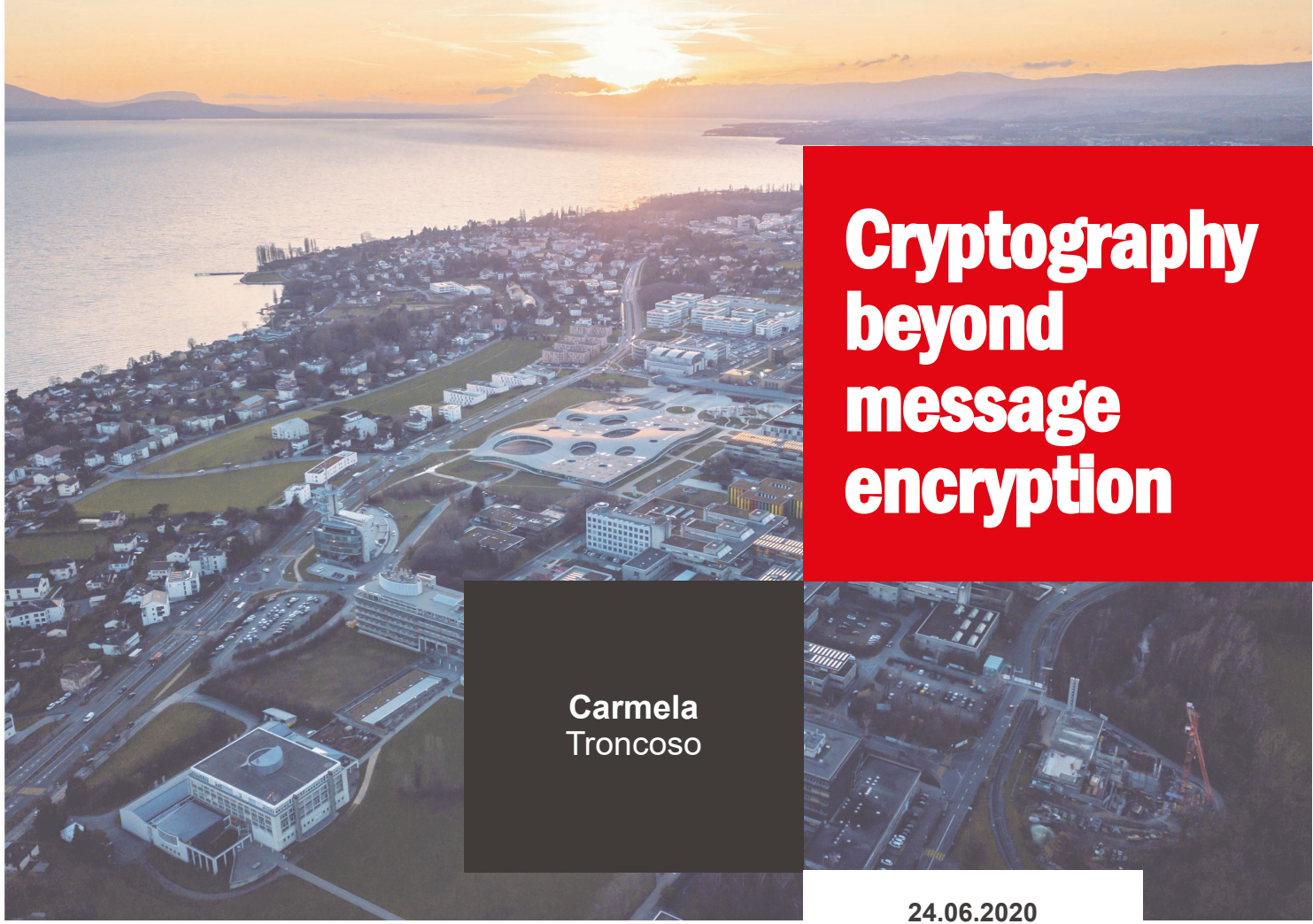
EPFL



Cryptography beyond message encryption

Carmela
Troncoso

24.06.2020

École
polytechnique
fédérale
de Lausanne

Example 1: Decentralized privacy-preserving proximity tracing

Decentralized Privacy-Preserving Proximity Tracing

Version: 25 May 2020.

Contact the first author for the latest version.

EPFL: Prof. Carmela Troncoso, Prof. Mathias Payer, Prof. Jean-Pierre Hubaux, Prof. Marcel Salathé, Prof. James Larus, Prof. Edouard Bugnion, Dr. Wouter Lueks, Theresa Stadler, Dr. Apostolos Pyrgelis, Dr. Daniele Antonioli, Ludovic Barman, Sylvain Chatel

ETHZ: Prof. Kenneth Paterson, Prof. Srdjan Čapkun, Prof. David Basin, Dr. Jan Beutel, Dr. Dennis Jackson, Dr. Marc Roeschlin, Patrick Leu

KU Leuven: Prof. Bart Preneel, Prof. Nigel Smart, Dr. Aysajan Abidin

TU Delft: Prof. Seda Gürses

University College London: Dr. Michael Veale

CISPA: Prof. Cas Cremers, Prof. Michael Backes, Dr. Nils Ole Tippenhauer

University of Oxford: Dr. Reuben Binns

University of Torino / ISI Foundation: Prof. Ciro Cattuto

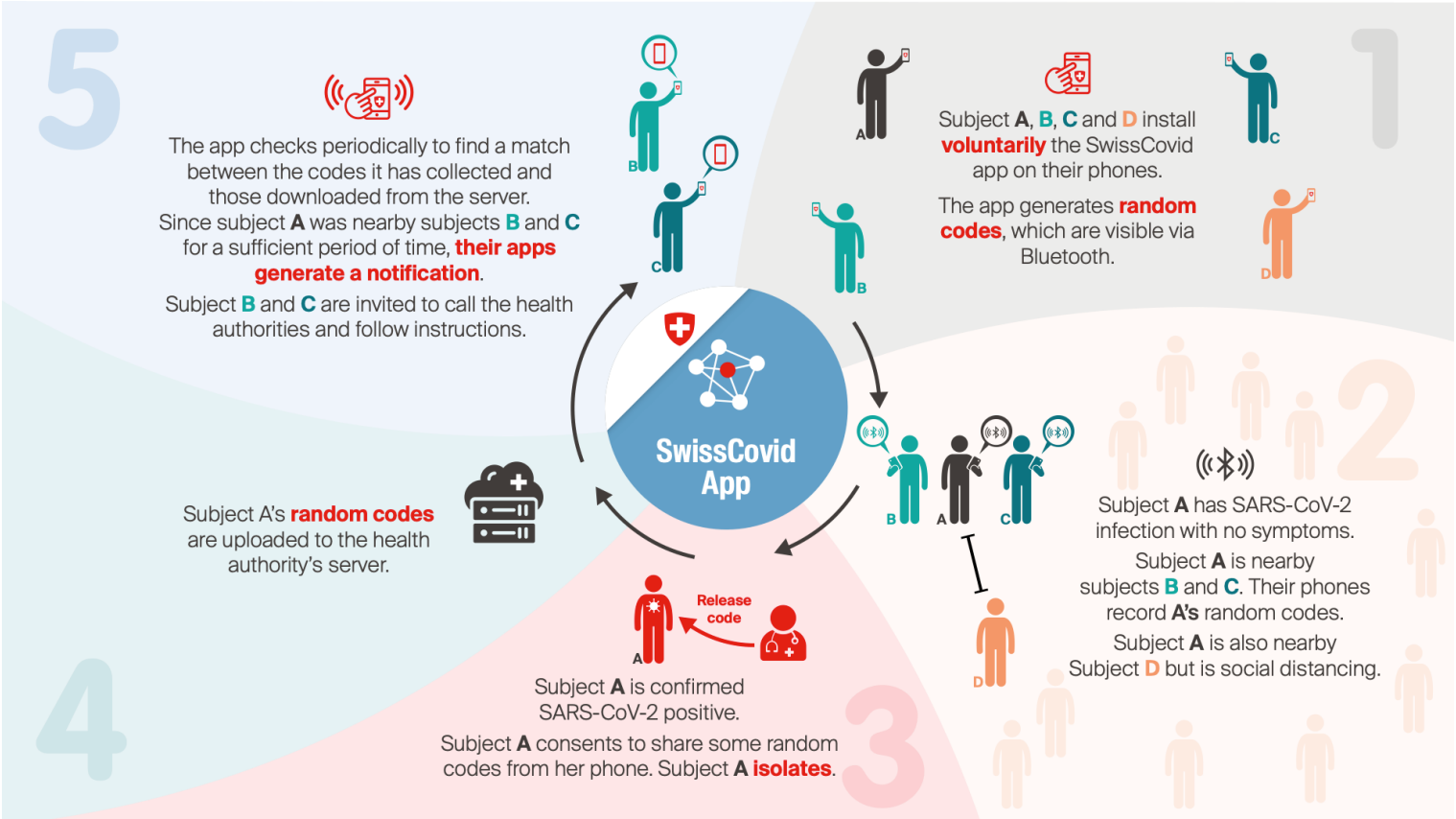
Aix Marseille Univ, Université de Toulon, CNRS, CPT: Dr. Alain Barrat

IMDEA Software Institute: Prof. Dario Fiore

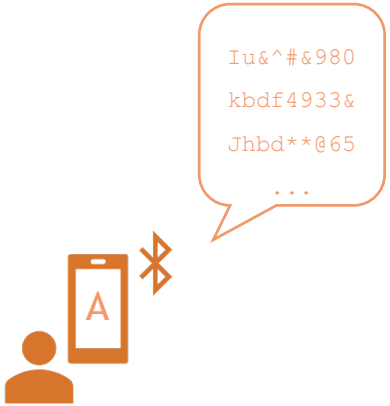
INESC TEC: Prof. Manuel Barbosa (FCUP), Prof. Rui Oliveira (UMinho), Prof. José Pereira (UMinho)

Carmela Troncoso

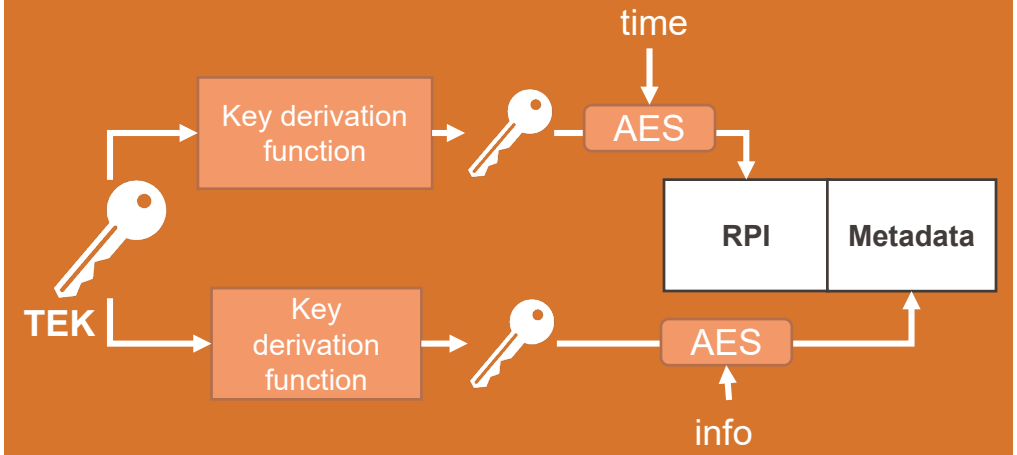
How it works



Cryptography as a support for privacy



- The App creates a **secret every day** (**TEK**) and from this key it derives **random identifiers (RPIs)** that it broadcasts via Bluetooth
- A random identifier is used for a limited amount of time
- Without the key, no-one can link two identifiers

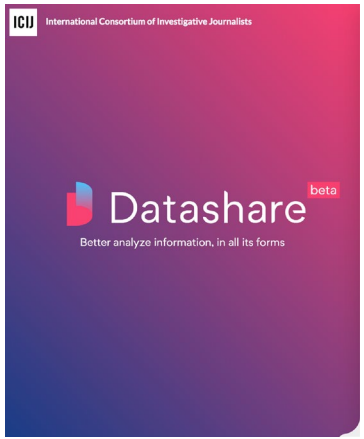


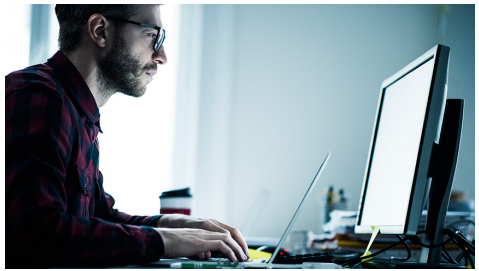
https://blog.google/documents/69/Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf

Example 2: Datashare Network
Decentralized search engine for journalists

EPFL

ICIJ The International Consortium of Investigative Journalists

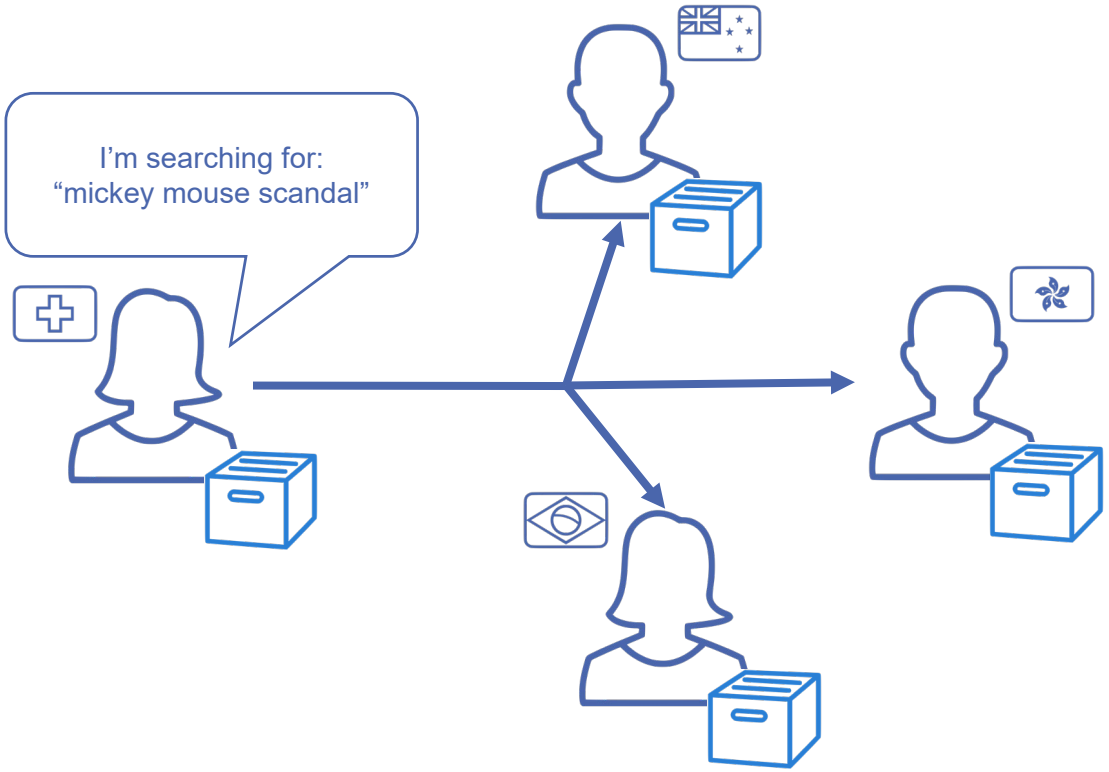




Datashare Network Goal

Journalists can search on others' collections for keywords of interest

- Only ICIJ and associates can use the system
- Query content is not revealed
- Searching is anonymous
- Journalists can anonymously converse with journalists that have matching documents



Authentication

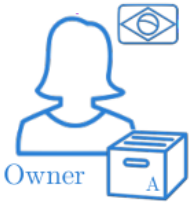
Journalists can search on others' collections for keywords of interest

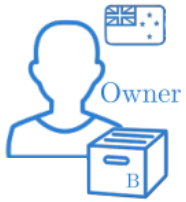
- **Only ICIJ and associates can use the system**

ATTRIBUTE-BASED CREDENTIALS

Prove attributes in "Zero-knowledge"

"I am a member of the organization"
Prove that you have a signature of the organization on a secret you only know





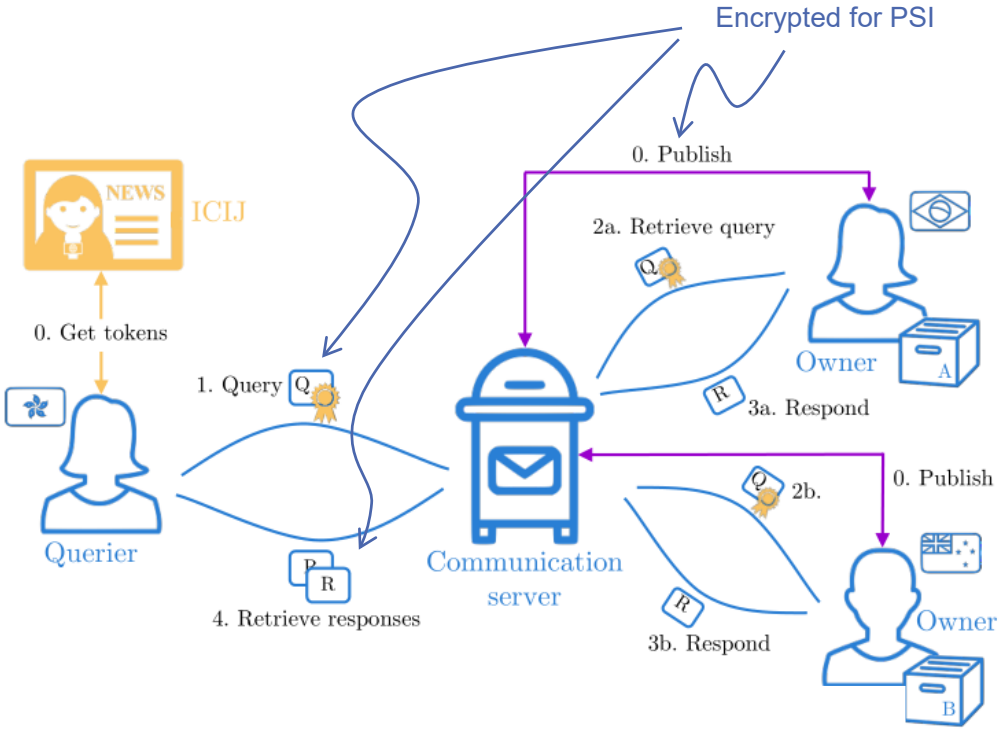
Search

Journalists can search on others' collections for keywords of interest

- **Query content is not revealed**

(Multi set) Private Set Intersection

Find (cardinality of) the intersection between two sets without learning anything about the rest of the elements



Anonymous communications

Journalists can search on others' collections for keywords of interest

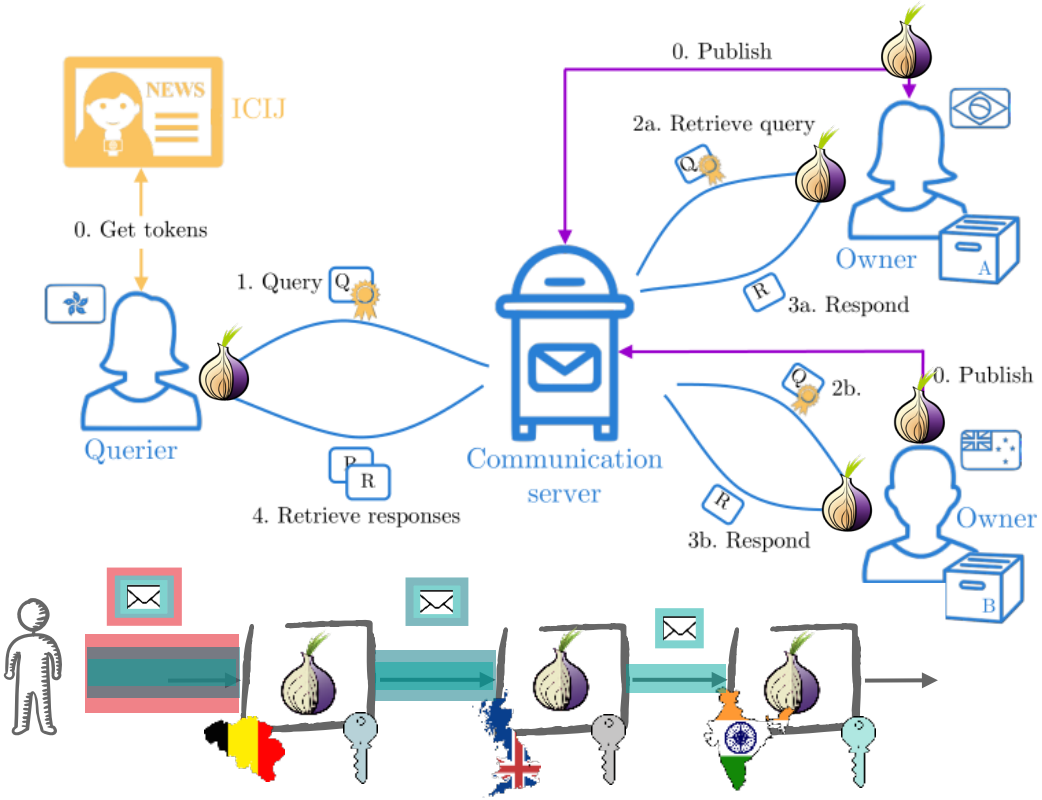
- **Searching is anonymous**

Anonymous Communications

Rerouting to hide IPs

Tor or Nym

Encryption not only hides content, also avoids tracing messages across routers



Anonymous messaging

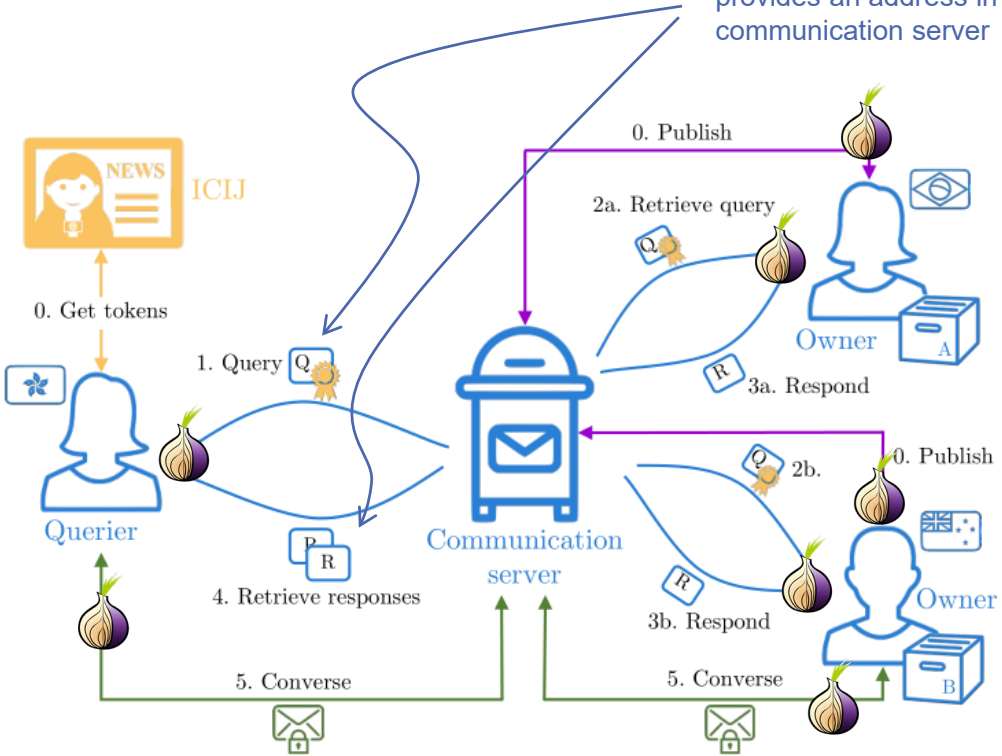
Journalists can search on others' collections for keywords of interest

- **Journalists can anonymously converse with journalists that have matching documents**

Anonymous Asynchronous Messaging

Cryptography to establish rendez-vous pigeonholes only known to conversation partners

Dummy messages (encrypted for indistinguishability)



Take away message

Encryption is a **KEY** tool for privacy, because it can do **MUCH MORE** than hiding the content of messages

Ensure **unlinkability**: messages, actions, authentications, of a user cannot be linked over time

Enable **anonymous authentication** while still providing guarantees against misuse

Enable **private search** and multi-party operations without revealing data

Provide **common knowledge** to bootstrap further private actions

EPFL

Thank you for your attention

Carmela
Troncoso

École
polytechnique
fédérale
de Lausanne