Anonymous communication

Boaz Barak

**Disclaimer:** The MS-Word version of this text has significant formatting issues compared to the PDF and HTML versions.

# Anonymous communication

Encryption is meant to protect the contents of communication, but sometimes the bigger secret is that the communication existed in the first place. If a whistleblower wants to leak some information to the New York Times, the mere fact that she sent an email would reveal her identity. There are two main concepts aimed at achieving anonymity:

* *Anonymous routing* is about ensuring that Alice and Bob can communicate without that fact being revealed.
* *Steganography* is about having Alice and Bob hiding an encrypted communication in the context of an seemingly innocuous conversation.

## Steganography

The goal in a stegnaographic communication is to hide cryptographic (or non cryptographic) content without being detected. The idea is simple: let’s start with the *symmetric case* and assume Alice and Bob share a shared key and Alice wants to transmit a bit to Bob. We assume that Alice and has a choice of words that would be reasonable for her to send at this point in the conversation. Alice will choose a word such that where is a pseudorandom function collection. With probability there will be such a word. Bob will decode the message using . Alice and Bob can use an error correcting code to compensate for the probability that Alice is forced to send the wrong bit.

In the *public key setting*, suppose that Bob publishes a public key for an encryption scheme that has *pseudorandom ciphertexts*. That is, to a party that does not know the key, an encryption is indistinguishable from a random string. To send some message to Bob, Alice computes and transmits it to Bob one bit at a time. Given the words , to transmit the bit Alice chooses a word such that where is a hash function modeled as a random oracle. The distribution of words output by Alice is uniform conditioned on . But note that if is a random oracle, then is going to be uniform, and hence indistinguishable from .

## Anonymous routing

* **Low latency communication:** Aqua, Crowds, LAP, ShadowWalker, Tarzan, Tor
* **Message at a time, protection against timing / traffic analysis:** Mix-nets, e-voting, Dining Cryptographer network (DC net), Dissent, Herbivore, Riposte

## Tor

Basic arhictecture. Attacks

## Telex

## Riposte