22
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.

22.1 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 k and Alice wants to transmit a bit b to Bob. We assume that Alice and has a choice of t words $w_1, \ldots, w_t$ that would be reasonable for her to send at this point in the conversation. Alice will choose a word w_i such that $f_k(w_i) = b$ where $\{f_k\}$ is a pseudorandom function collection. With probability $1 - 2^{-t}$ there will be such a word. Bob will decode the message using $f_k(w_i)$. Alice and Bob can use an error correcting code to compensate for the probability 2^{-t} that Alice is forced to send the wrong bit.

In the *public key setting*, suppose that Bob publishes a public key e 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 m to Bob, Alice computes $c = E_e(m)$ and transmits it to Bob one bit at a time. Given the t words $w_1, \ldots, w_t$, to transmit the bit c_j Alice chooses a word w_i such that $H(w_i) = c_j$ where $H : \{0,1\}^* \to \{0,1\}$ is a hash function modeled as a random oracle. The distribution of words output by Alice $w^1, \ldots, w^\ell$ is uniform conditioned on $(H(w^1), \ldots, H(w^\ell)) = c$. But note that if H is a random oracle, then $H(w^1), \ldots, H(w^\ell)$ is going to be uniform, and hence indistinguishable from c.

22.2 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

22.3 TOR

Basic arhictecture. Attacks

22.4 TELEX

22.5 RIPOSTE

V

CONCLUSIONS