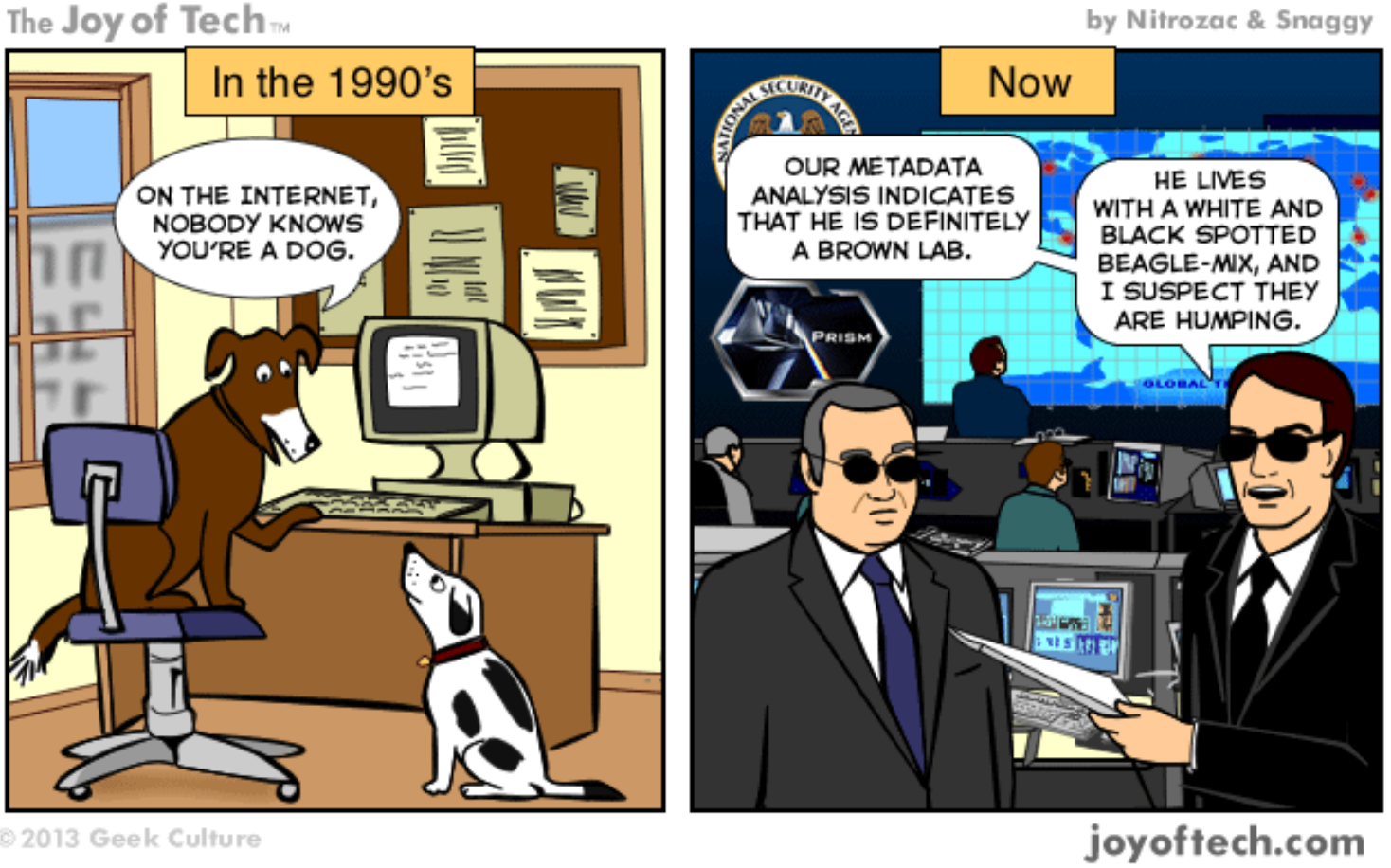
Onions and Garlic: the protocols of I2P

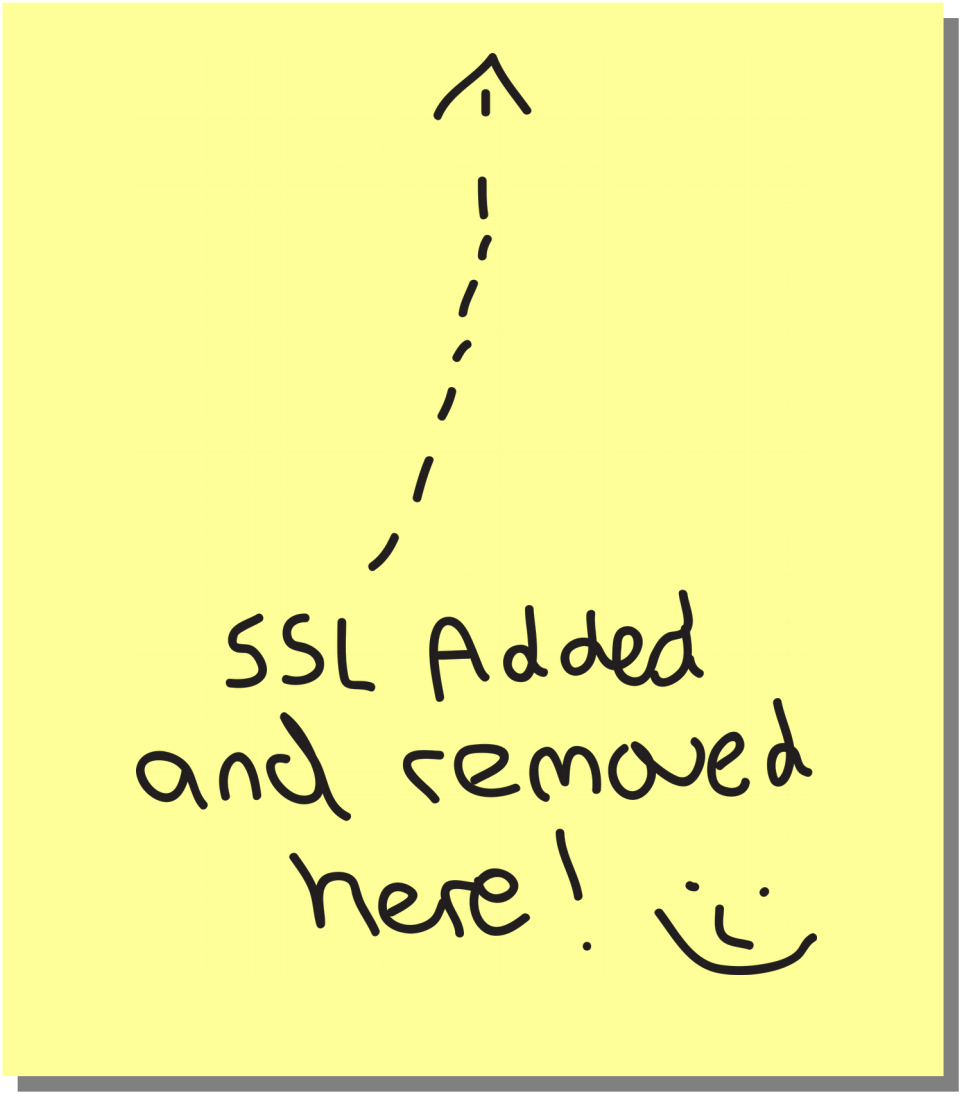
Jack Grigg
https://geti2p.net
str4d@i2pmail.org
Twitter: @str4d

2016-02-17

The Internet is not anonymous



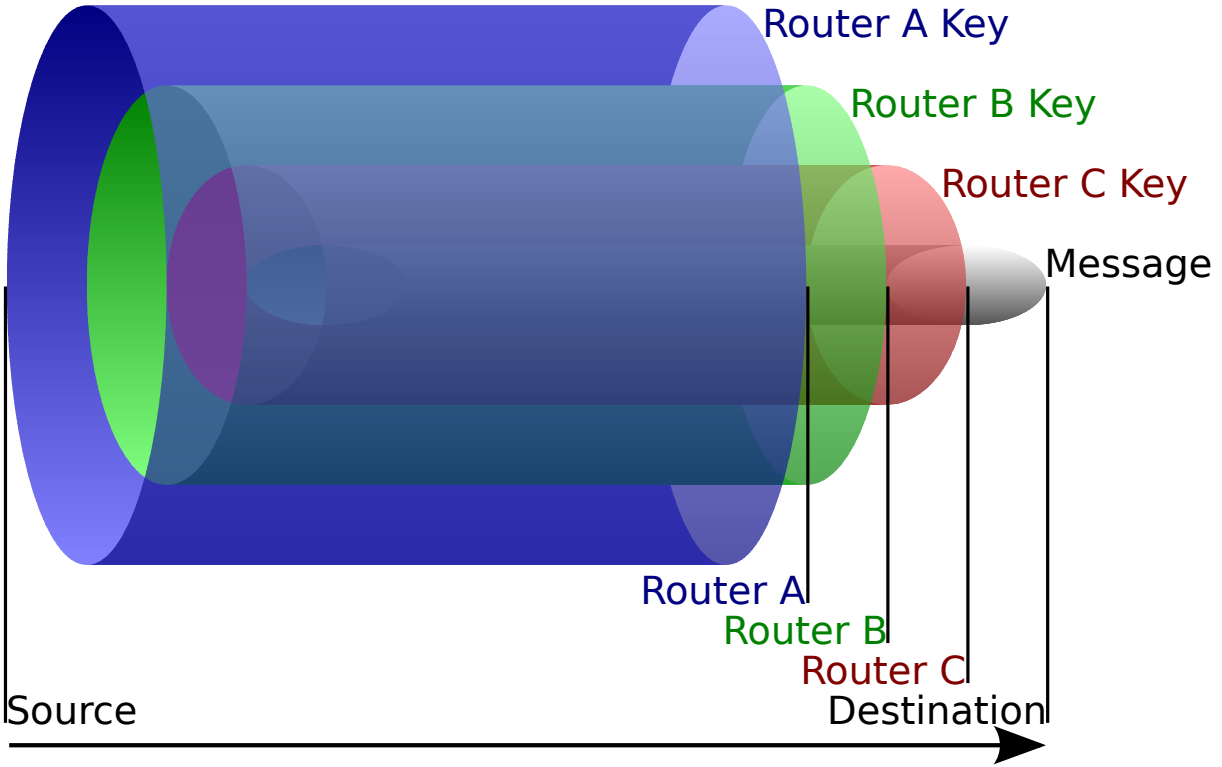
Standard protocols are insufficient



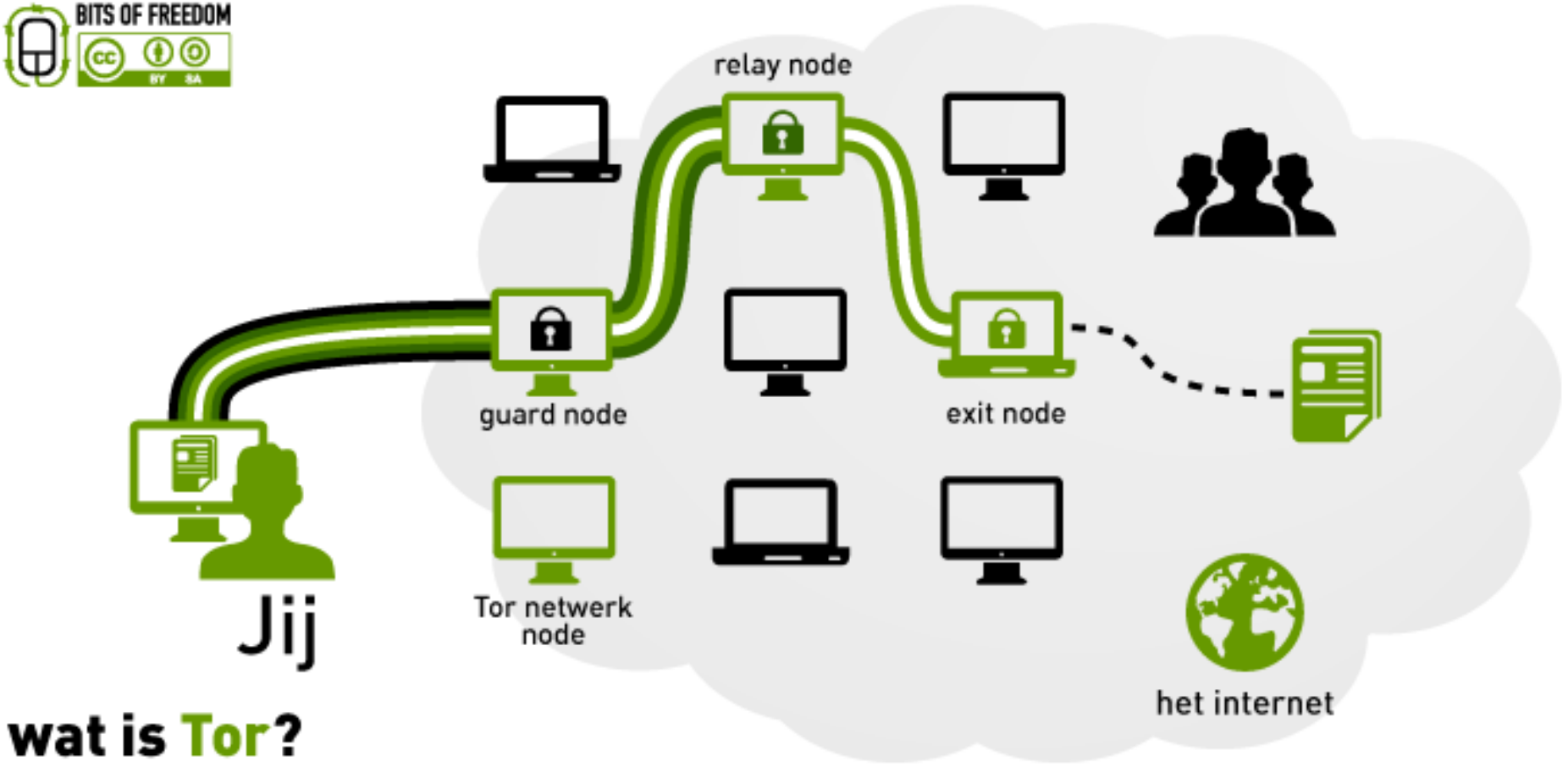
Types of anonymity systems

- Proxy services
- VPNs
- Mixnets
- DC nets
- DHT-based
- Onion routing ⟵

Onion routing



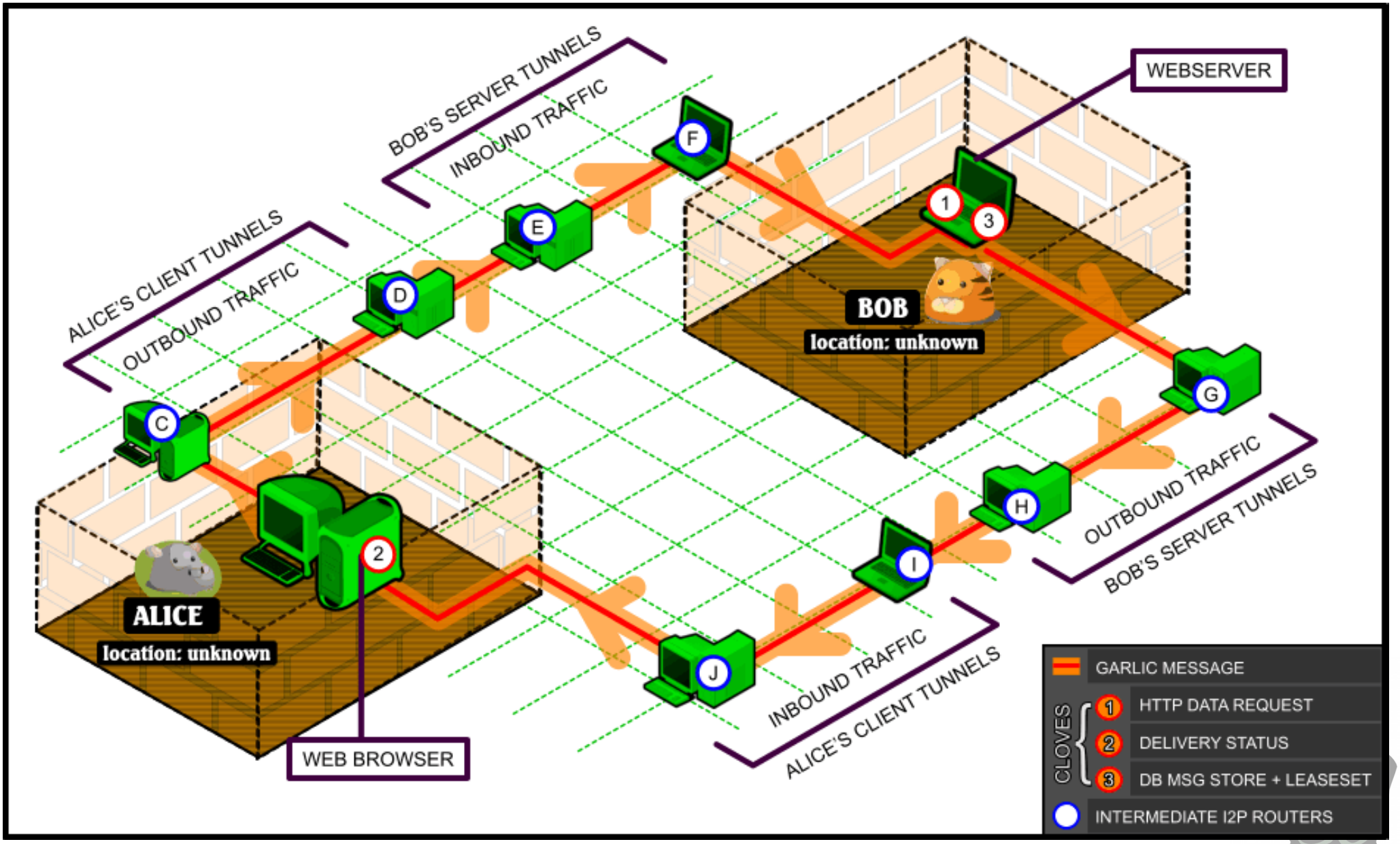
A simple example: Tor clients



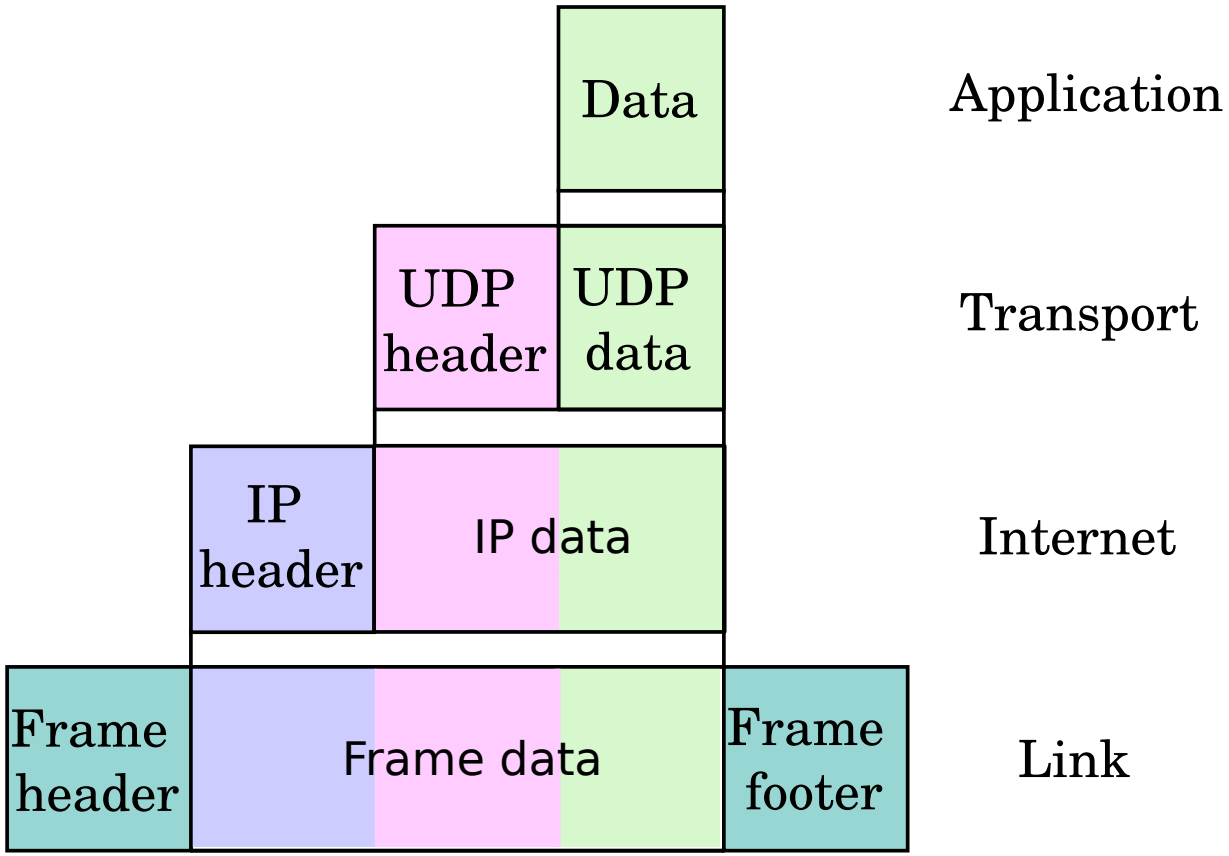
More fun: Tor Onion Services

- Connect two circuits together
  - Rendezvous Point
- Server gets the same protections
- Server addresses are self-authenticating

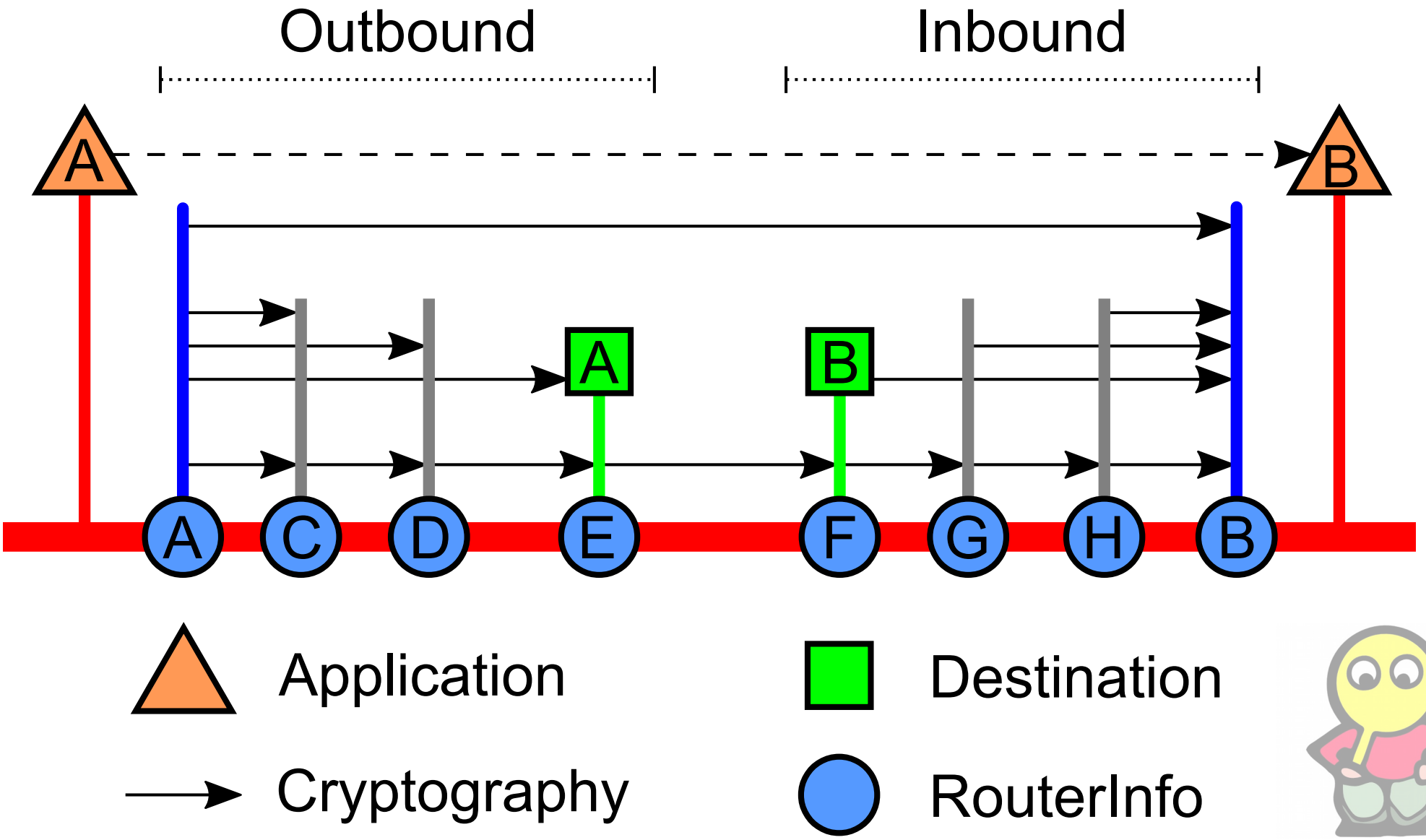
Even more fun: I2P



TCP/IP protocol stack



I2P inserts three protocol layers



I2P protocol stack

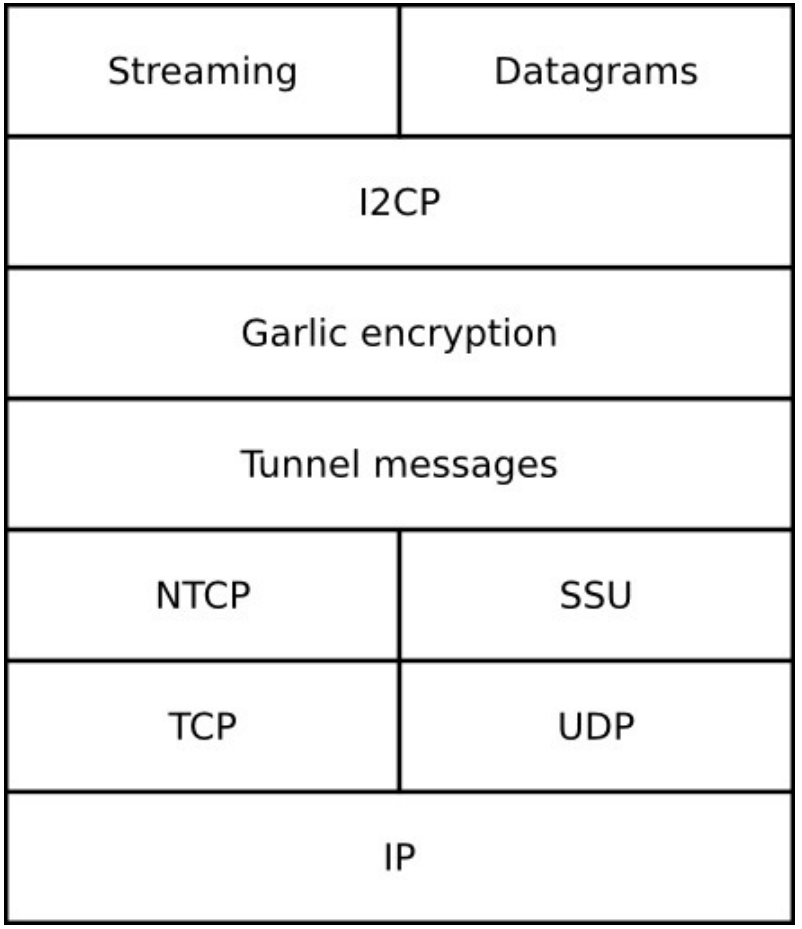
“Anonymous” data layer

End-to-end layer

Tunnel layer

Transport layer

TCP/IP layers



Analogues of TCP and UDP inside I2P

Onion routing only provides location anonymity!

(and even that is conditional)

I2P Network Protocol (I2NP)

- Manages routing and mixing of messages
  - Network database management
  - Tunnel building
  - Data transmission
- Each message is point-to-point
  - But can be combined in various ways

Transport layer

- Provides router-to-router delivery of I2NP messages
- Encrypts communication between routers
  - Secure 2-way-authenticated channel
- Provides confidentiality, not anonymity

Transport layer: transport types

- NTCP
  - TCP-based
  - Uses existing TCP stack for reliability
- SSU
  - UDP-based
  - Congestion control similar to TCP
    - Per-message retransmissions
    - Unique non-sequential identifiers → bitfields
  - Cooperative NAT/firewall traversal

Tunnel layer: build protocol

- A TunnelBuild message is repeatedly decrypted and forwarded between hops
  - “Non-interactive” telescopic tunnel building
  - Hops don't learn their location
- Each hop inserts their response into the packet
  - Agree to route data for next 10 minutes
  - Reject (e.g. bandwidth limits)
- Packet is returned via an existing tunnel

Tunnel layer: TunnelData messages

- Used for sending data through a tunnel
  - Onion-encrypted
- Fixed size (1028 kB)
  - Contain fragmented I2NP messages
- Delivery instructions per message

End-to-end layer: Garlic messages

- Used for sending data between peers
- Contain one or more GarlicCloves
  - each with its own delivery instructions

Flexible routing design

- Possible to implement a variety of mixnet delivery mechanisms
  - Garlics containing Cloves containing Garlics...
  - Combine with unused delay option in TunnelData delivery instructions
- Different trade-offs for different use cases
  - More research required!

Limitations

- No “exit nodes” at network level
  - Requires developer buy-in
- Implemented as an overlay network
  - Higher overhead
  - c/f stateless designs like HORNET
- More research required
  - Congestion control tuning
  - Designing next-gen protocols

Questions?

Network data structures