Darknets (Freenet, Tor, I2P)

- Was ist ein Darknet?
- Wofür braucht man es?
  - Anonymität im Internet
  - Zensierende Staaten
  - Jedem dritten wird der freie Internetzugang verwehrt
  - Great Firewall of China

Gliederung

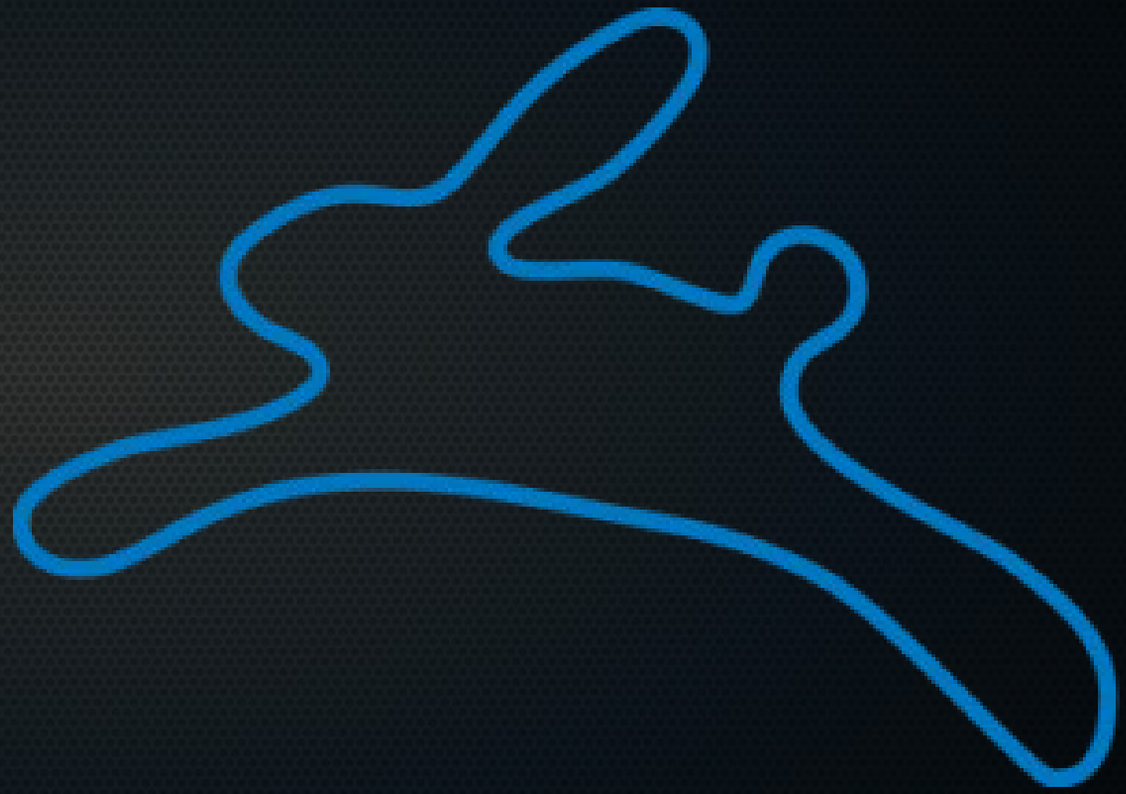
- Freenet
- Tor
- I2P

Freenet - Überblick

- Allgemein
- Routing
- Daten herunterladen
- Daten hochladen
- Speichersystem

Freenet - Allgemein

- Verteiltes System zur Speicherung und zum Abrufen von Informationen
- Ursprüngliche Idee von Ian Clarke (Universität Edinburgh)
- Peer-to-Peer-Netzwerk von Knoten, die die Freenet Software installiert haben



Freenet - Allgemein

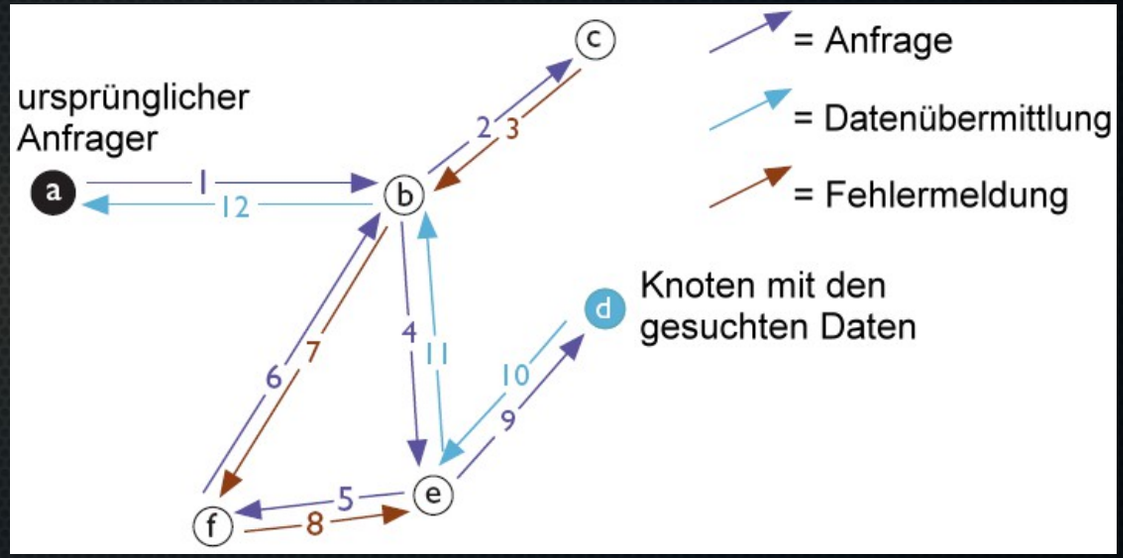
- Jeder Knoten hat eigenen Datenspeicher
- Wird dem Netzwerk für Lese- und Schreibzugriffe zur Verfügung gestellt
- Garantiert keine keine permanente Speicherung (näheres später)
- Bietet nur Anonymität innerhalb des Netzwerkes

Freenet - Routing

- Knoten und Dateien sind mit einer Location ϵ [0,1) verknüpft
- Knoten verwalten Routingtabelle (DHT)
  - Zuordnung von Knoten zu Daten
- Routingentscheidungen basierend auf Abstand von Locations
- Bsp.: Suche nach Schlüssel mit Location 0,4
  - Routingtabelle mit Einträgen für 0,6 und 0,7
  - 0,6 näher

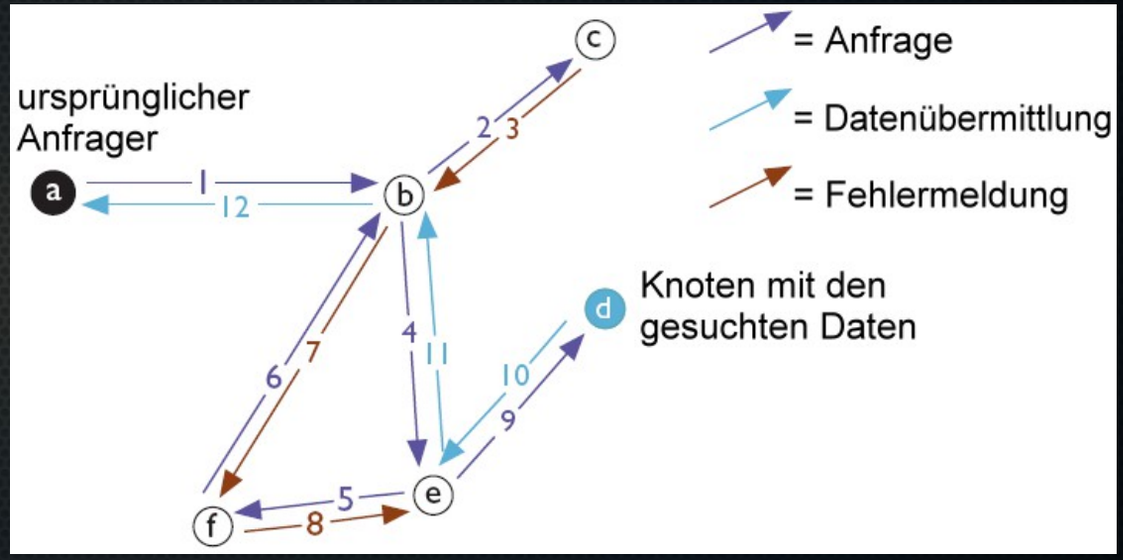
Freenet – Daten herunterladen

- Request an lokalen Knoten
  - Hops to live (HTL)
  - gesuchter Schlüssel
- Algorithmus:
  - Überprüfe eigenen Speicher
  - Vorhanden ? → zurückliefern
  - Sonst: Weiterleitung an ähnlichen Knoten
- Etablierte Kette: (a, b, e, d)



Freenet – Daten hochladen

- Request an lokalen Knoten
  - Hops to live (HTL)
  - berechneter Schlüssel
- Gleicher Algorithmus
  - Datei gefunden → Schlüsselkollision
  - Ansonsten Ausbau der Kette
  - Replikation der Datei entlang der Kette



Freenet - Speichersystem

- Problem: Speicherplatz ist endlich
- Daten werden nach dem LRU Prinzip gelöscht
  - Am längsten nicht verwendeten Dateien werden gelöscht
- Daten sind verschlüsselt (Rijndael 256-Bit)
  - Bestreitbarkeit

Freenet - Darknet vs Opennet

- Version 0.7: Idee eines Friend-to-Friend-Netzwerk kam auf (Darknet)
- Kommunikation auf Freunde (trust peers) beschränkt
- Daten aber immer noch global verfügbar
- Ebenso Hybrid-Modell, in dem Knoten ihre Identität auch an Unbekannte weitergeben (Opennet)

Freenet - Evaluation

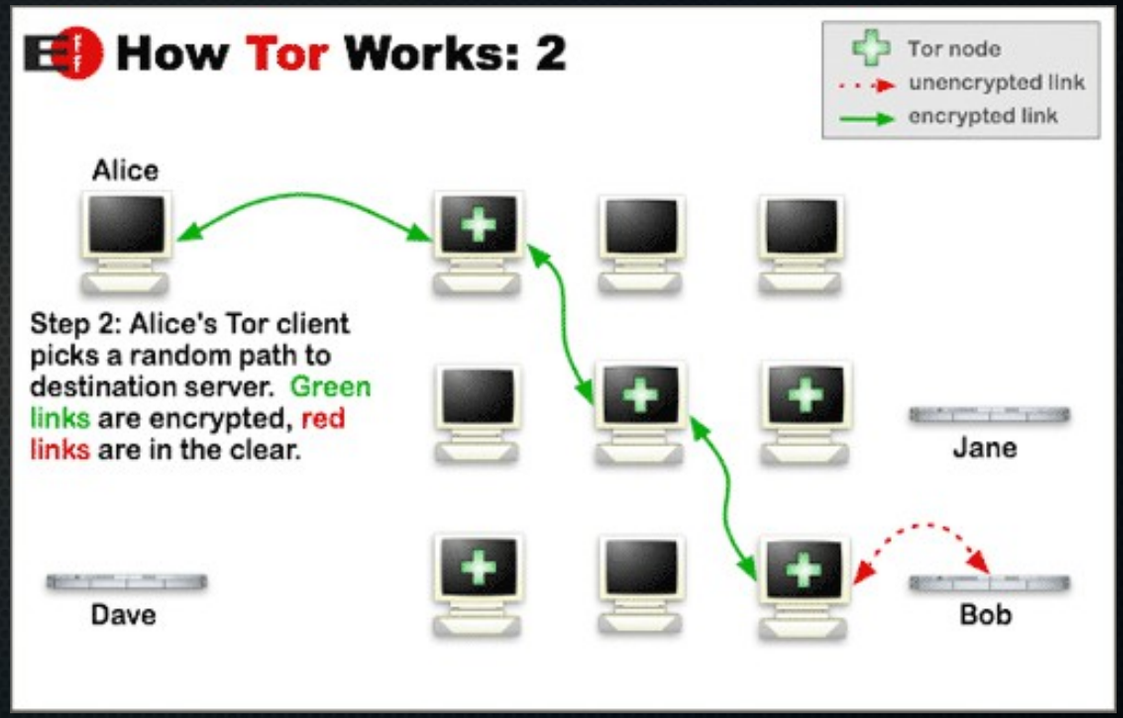
- Harvesting trotz dezentralen Struktur
  - Sammeln der IP-Adressen der Freenet Knoten
- China hat 2005 Freenet geblockt
- Harvesting nur in Opennet möglich
- Dateien sind noch verfügbar, wenn Uploader offline

Tor - Überblick

- Allgemein
- Directory Servers
- Hidden Services

Tor - Allgemein

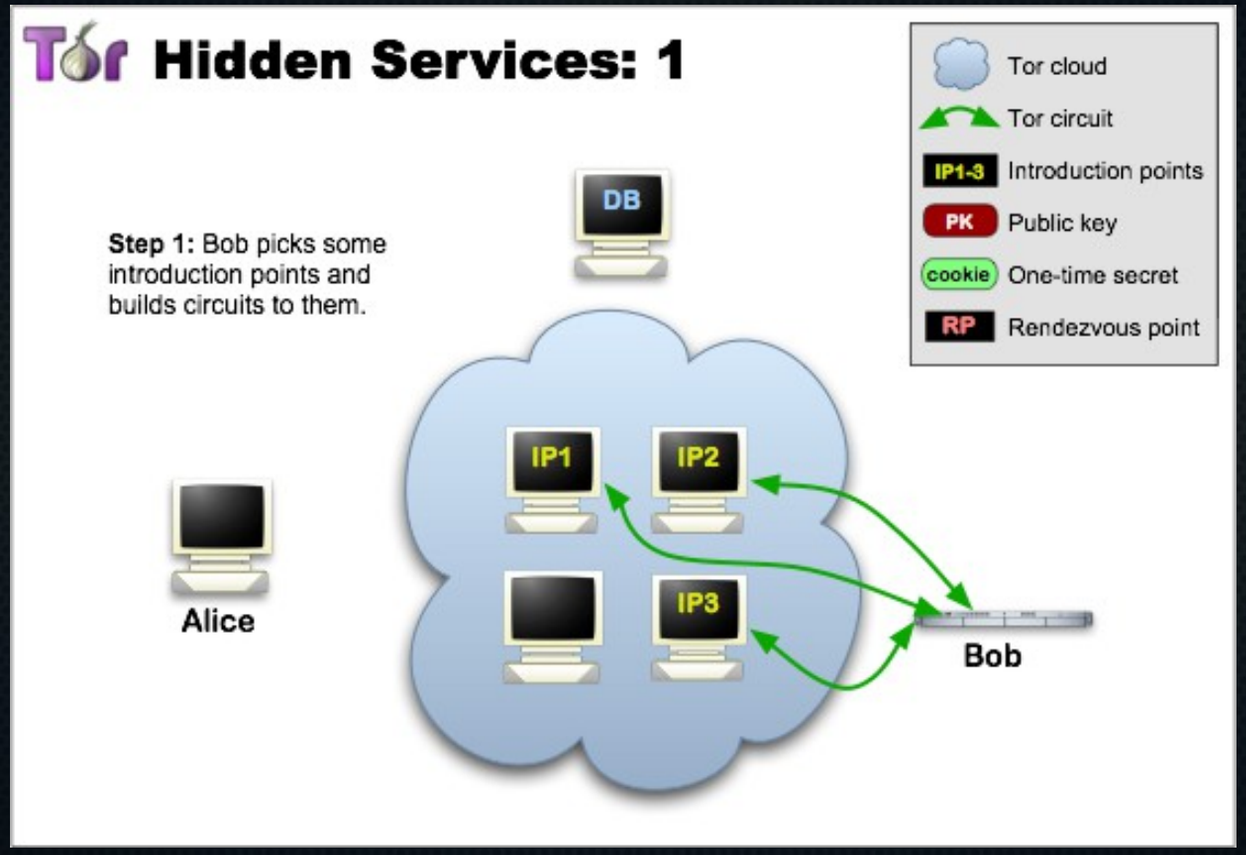
- 2nd Generation Onion Routing
- Ursprung bei Naval Research Laboratory (USA)
- Mitentwicklung durch einen der Erfinder des ursprünglichen Onion Routing (Paul Syverson)
- Overlay-Netzwerk, das TCP-Verbindungen anonymisiert
- Für Echtzeitkommunikation geeignet
- Ähnlich zu Java Anon Proxy (JAV), Mixkaskade von Proxies



Tor - Directory Server

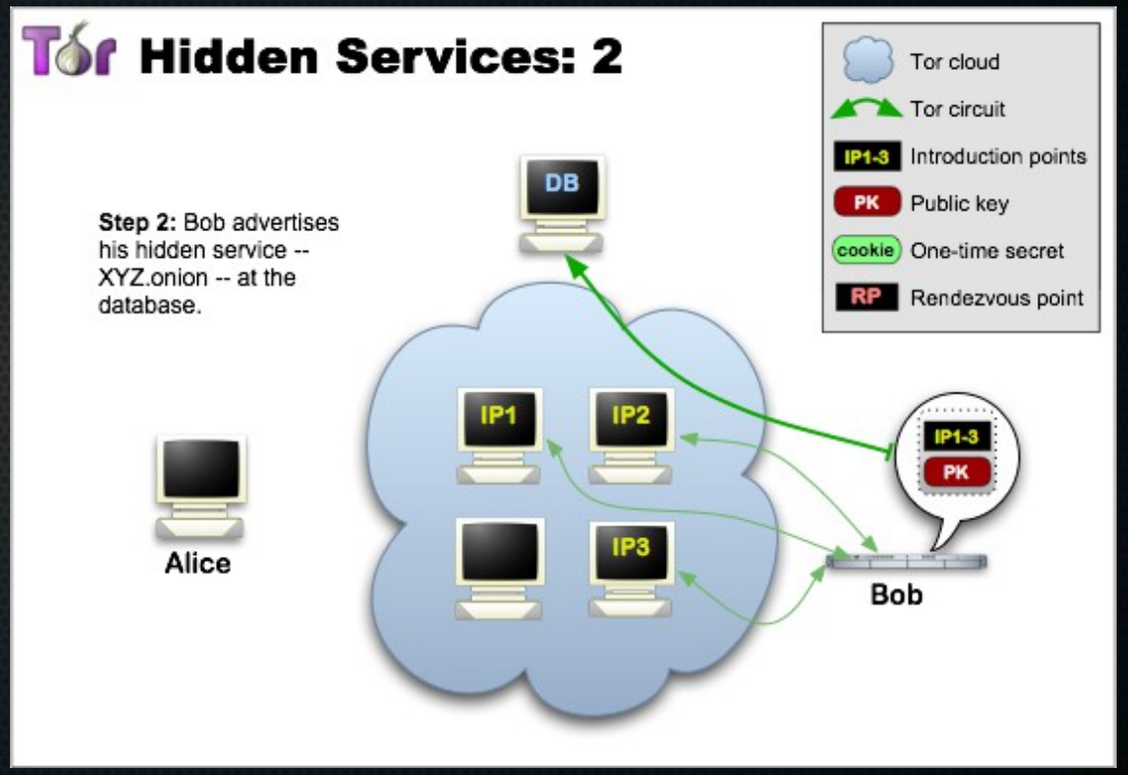
- Liefert Signed Directory von Onion Routern via HTTP
  - Adresse des Onion Router
  - Öffentlicher Schlüssel
  - Exit Policies
- Signed Directories werden von Onion Routern selbstständig veröffentlicht
- Server synchronisieren sich untereinander

Tor - Hidden Services 1



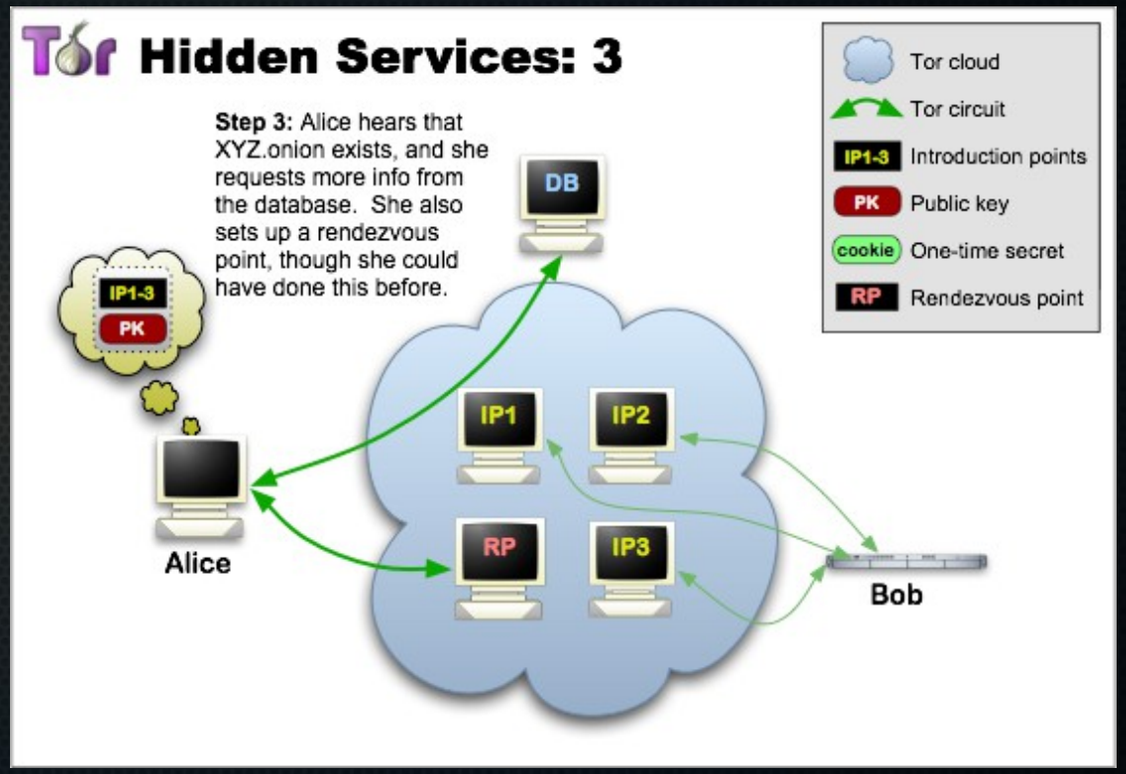
Tor - Hidden Services 2

- Bob macht seinen Dienst bekannt:
  - Öffentlicher Schlüssel
  - Introduction Points
- Wird als Service Descriptor in einer Distributed-Hash-Table hinterlegt



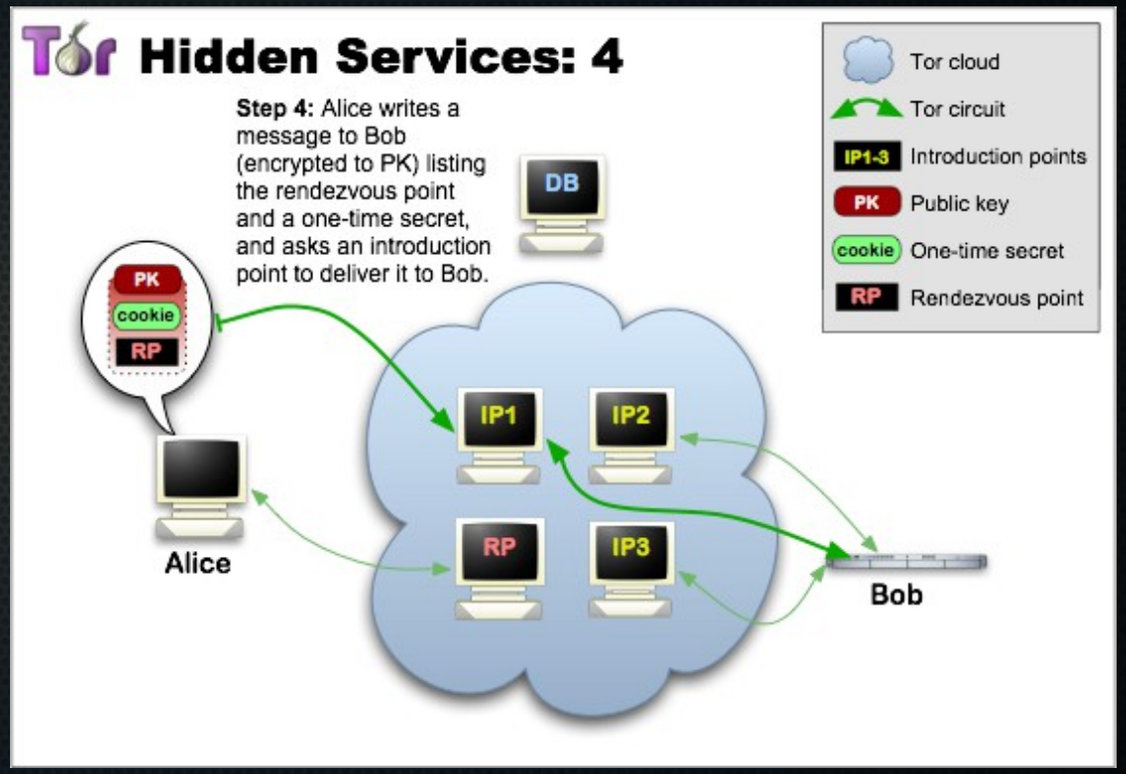
Tor - Hidden Services 3

- Alice baut Circuit zu Rendezvous Point
- Hinterlässt Rendezvous Cookie (one-time secret)



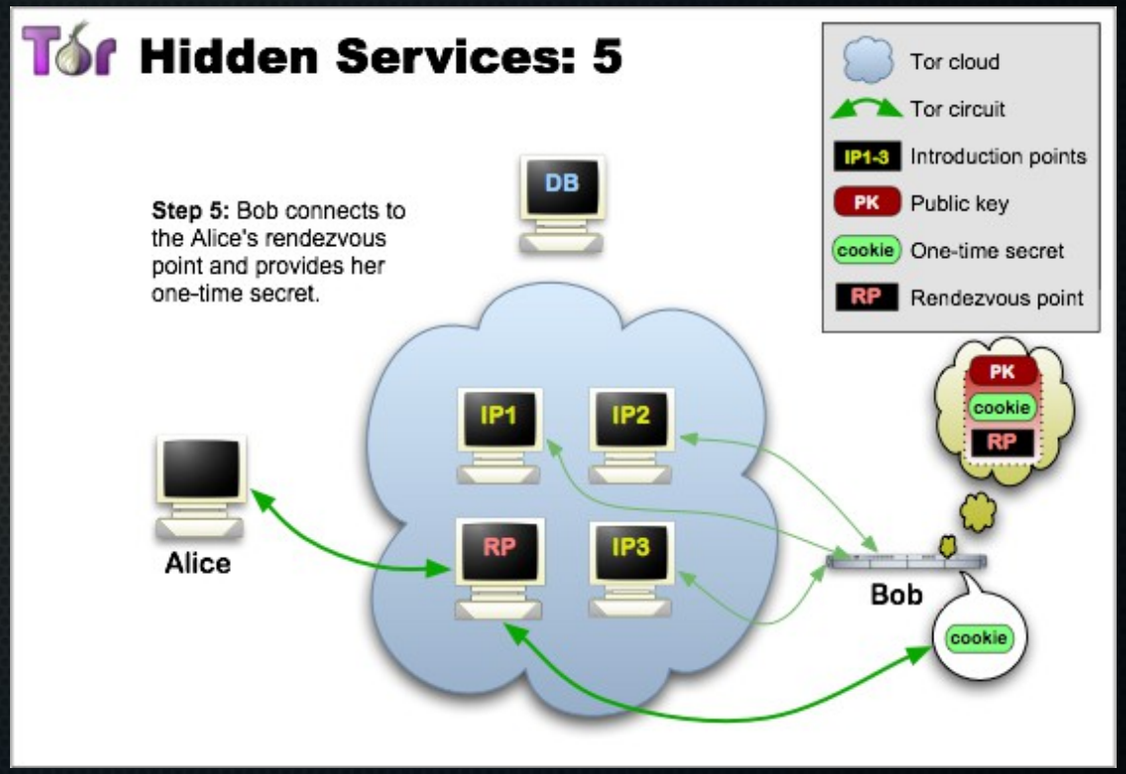
Tor - Hidden Services 4

- Alice baut Verbindung zu einem Introduction Point auf
- Hinterlässt Nachricht mit
  - Rendezvous Cookie
  - Rendezvous Point
  - Hälfte DH Handshake
- Verschlüsselt mit Bobs PK



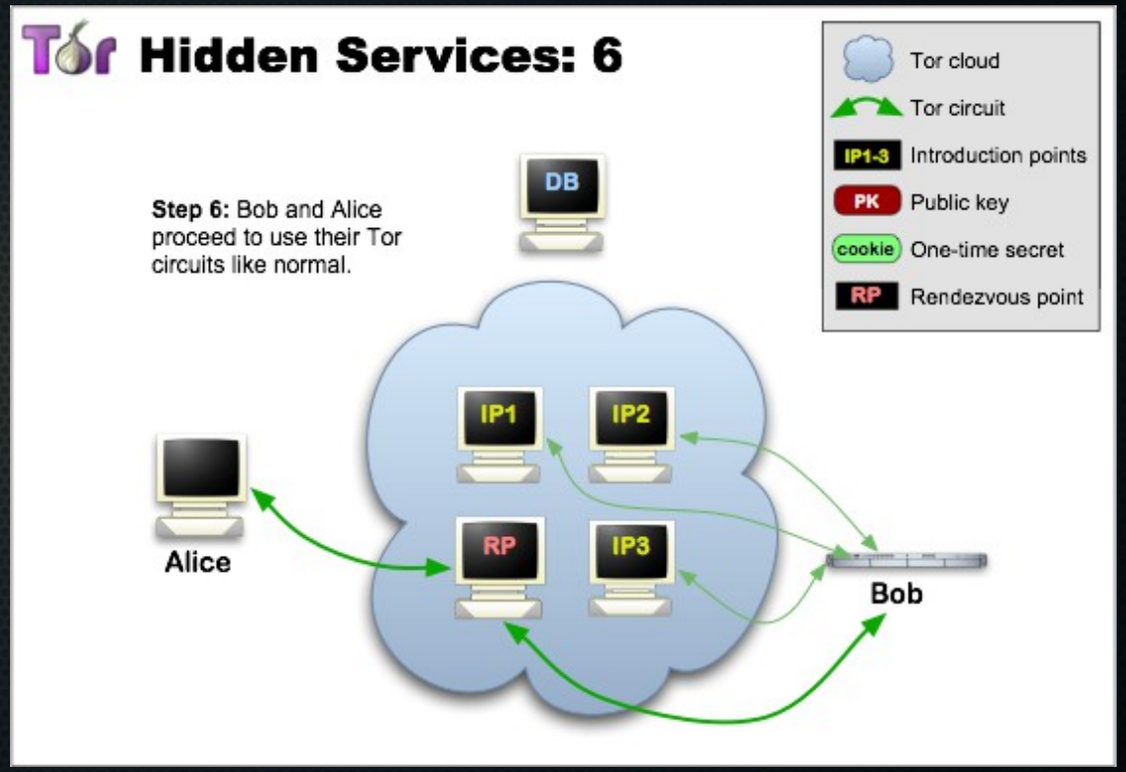
Tor - Hidden Services 5

- Bob baut Circuit zu RP auf
- Antwortet mit
  - zweiten Hälfte des DH Handshakes
  - Hash des ausgehandelten Schlüssels



Tor - Hidden Services 6

- Die Circuits wurden miteinander verbunden:
  - Alice ↔ Rendezvous Point
  - Introduction Point ↔ Bob



Tor - Evaluation

- Gefährlich: Plugins wie Flash
  - Können IP enthüllen
  - Tor Browser Bundle speziell dafür angepasst
- Exit Node Missbrauch
  - Sieht Nachricht in plaintext
  - Besser keine sensiblen Daten über Tor senden
- Zentrale Directory Server → Blockiert von China
  - Bridge Relays

I2P - Überblick

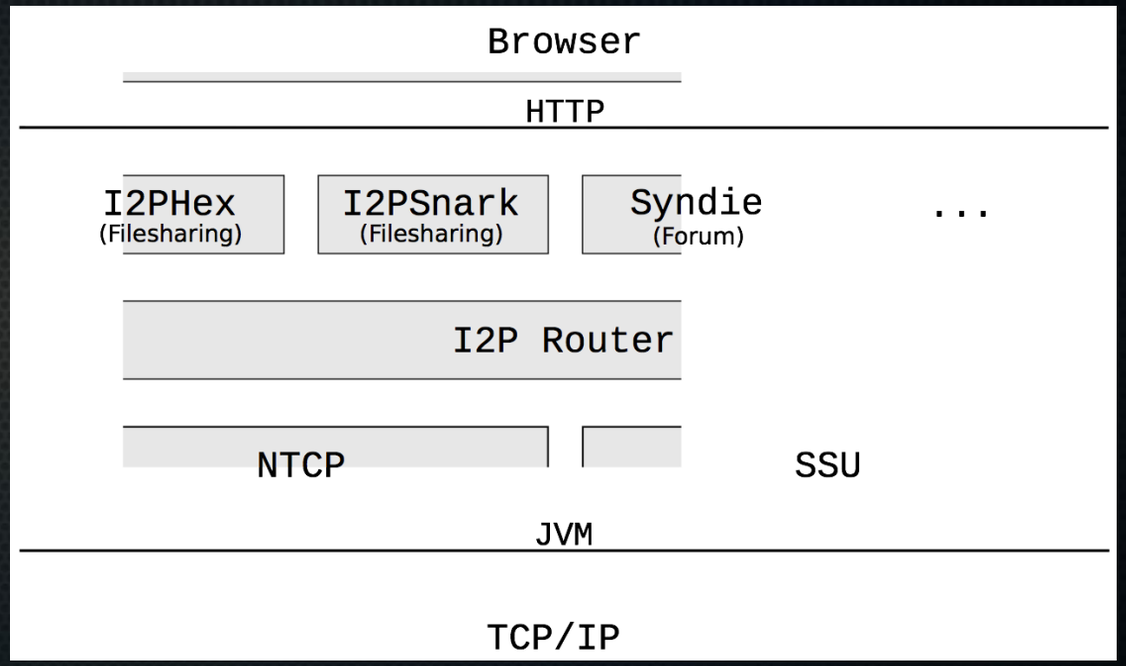
- Allgemein
- Tunnel
- NetDb
- Kommunikation

I2P - Allgemein

- Steht für Internet Invisible Project
- Wie Tor low latency network
- Entwickler anonym
- Hauptentwickler: jrandom
- Komplett dezentralisiert
- Basiert nicht auf zentralen Strukturen wie Directory Server

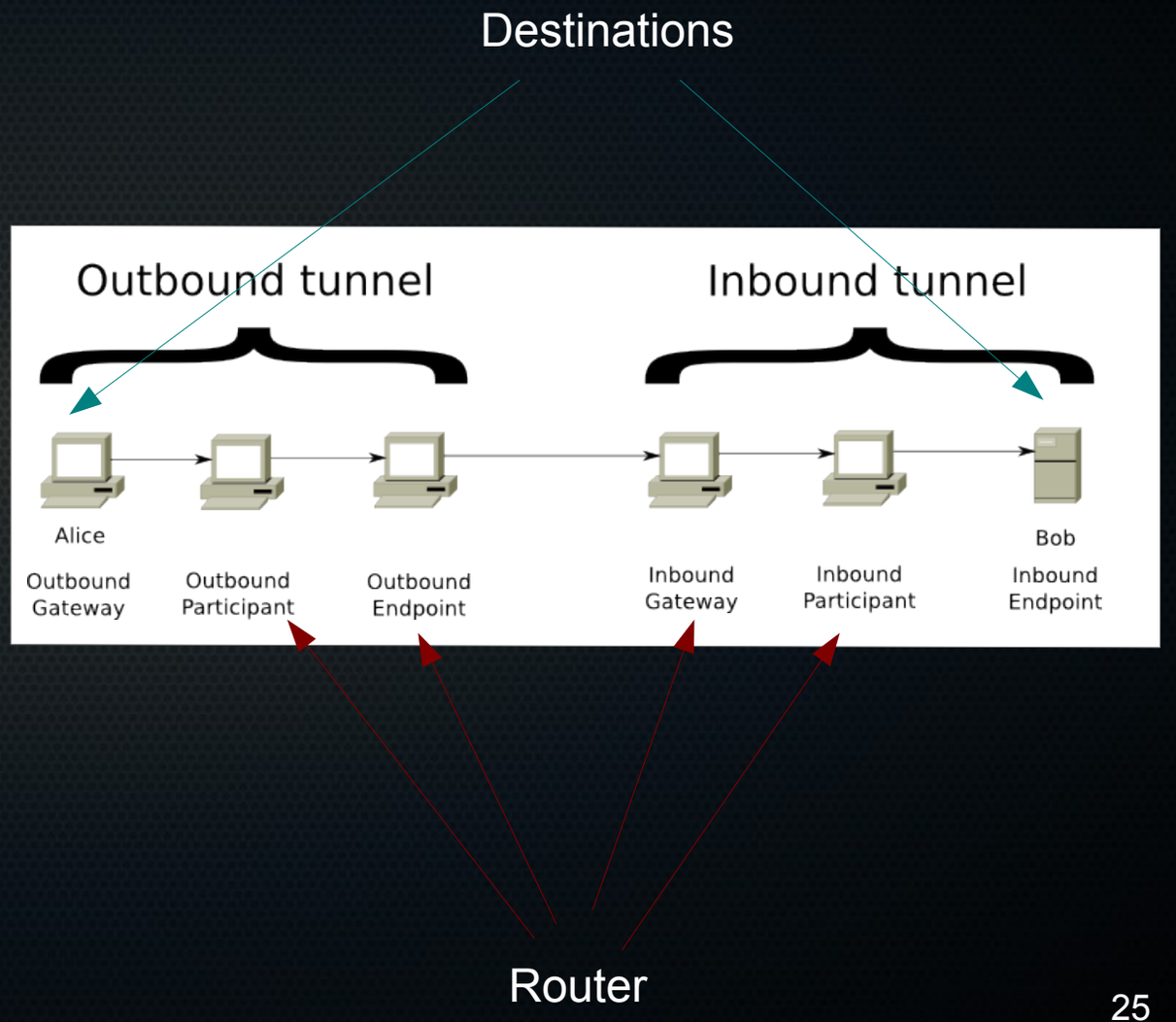
I2P - Allgemein

- Eigenständiges Netzwerk
- Anonyme Kommunikation nur innerhalb dessen
- Speziell auf I2P angepasste Applikationen basierend auf I2P APIs
- Bietet TCP (NTCP) und UDP (SSU)



I2P - Tunnel

- Kommunikation durch Tunnel
- Tunnel sind unidirektional
- Client Tunnel
  - Outbound und Inbound Tunnel
- Exploratory Tunnel
- Destinations und Router

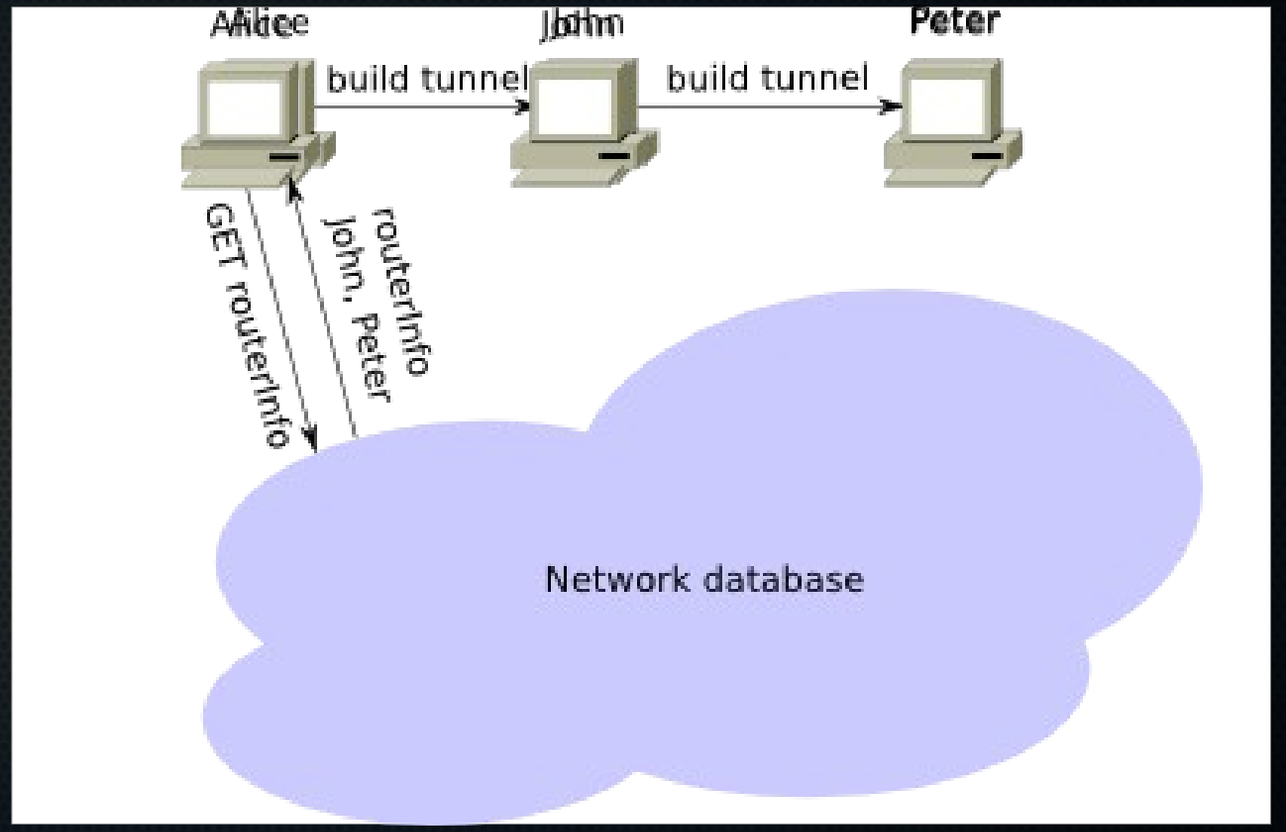


I2P - NetDB

- Verteilte Datenbank (DHT), verwaltet von Floodfill Router
- Enthält Informationen wie Router und Destinations zu erreichen sind
  - RouterInfo
  - LeaseSet
- Anfragen an netDB durch Exploratory Tunnel

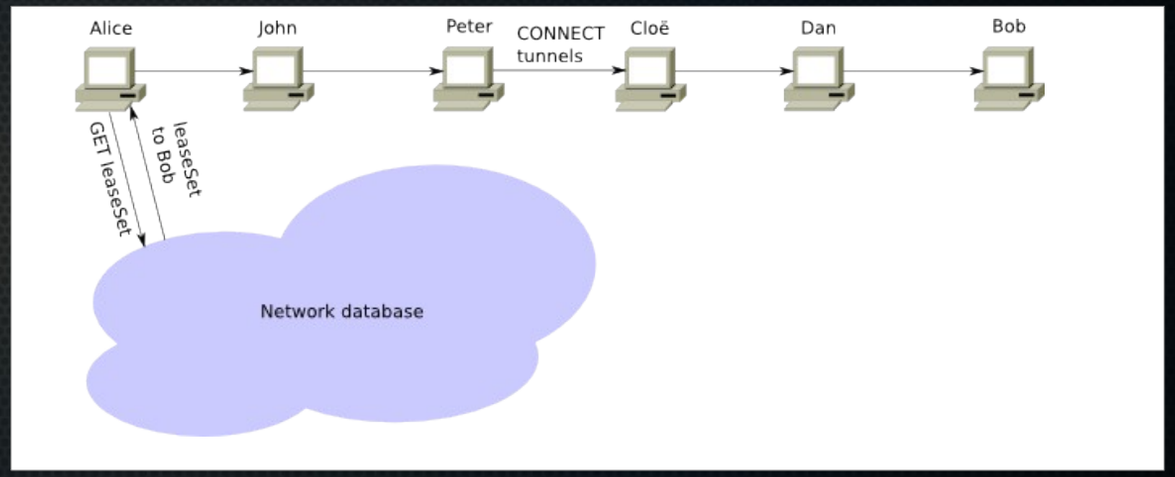
I2P - Tunnelerstellung

- Bekannte Router werden erfragt (netDB)
- Kategorisierung von Routern nach Performanz etc.
- Tunnel wird erstellt

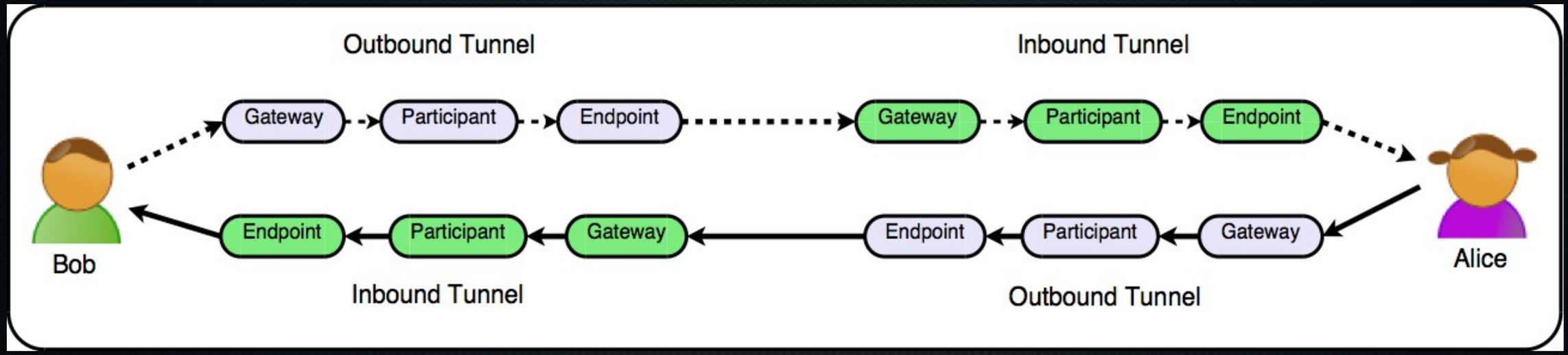


I2P - Kommunikation

- Tunnel sind erstellt
- Inbound Tunnel durch LeaseSet der NetDB bekannt
- Nachricht mit Instruktionen an Peter, an Cloé weiterzusenden
- Schichtweise Verschlüsselung
- Zusätzlich Ende-zu-Ende-Verschlüsselung (Garlic Encryption)



I2P - Vollständige Kommunikation



I2P - Evaluation

- In sich geschlossenes Netzwerk
- Vermeidet SOCKS Proxy Interface
  - I2P APIs
- Garlic Encryption
- I2P speziell für Hidden Services konzipiert
- Abhören der Kommunikation erfordert Kompromittierung von doppelt so vielen Knoten
  - Unidirektionale Tunnel

Zusammenfassung

- Freenet → Verteilter Datenspeicher
- Tor → Anonymisierung des Internetverkehrs
- I2P → Eigenständiges Netzwerk