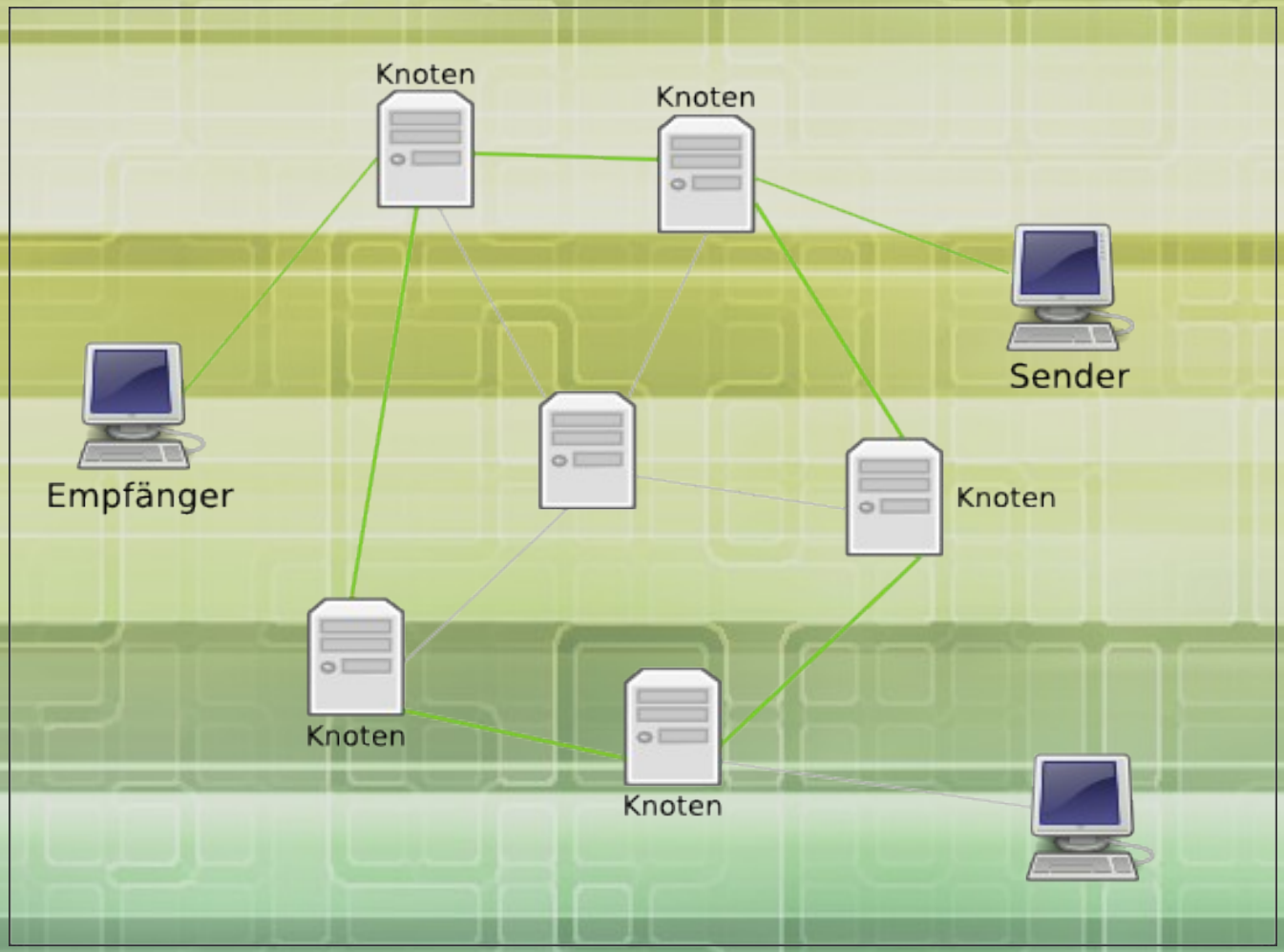
Crypto-Seminar

- sichere Email-Kommunikation
  - Warum ist das Internet anfällig für Überwachung?
  - Sicher kommunizieren in unsicheren Netzwerken?
  - Wie funktioniert asymmetrische Verschlüsselung?
- sicher surfen im WWW
  - Wie funktioniert Onion-Routing?

sense.lab

Internet



sense.lab

Warum ist das Internet anfällig für Überwachung?

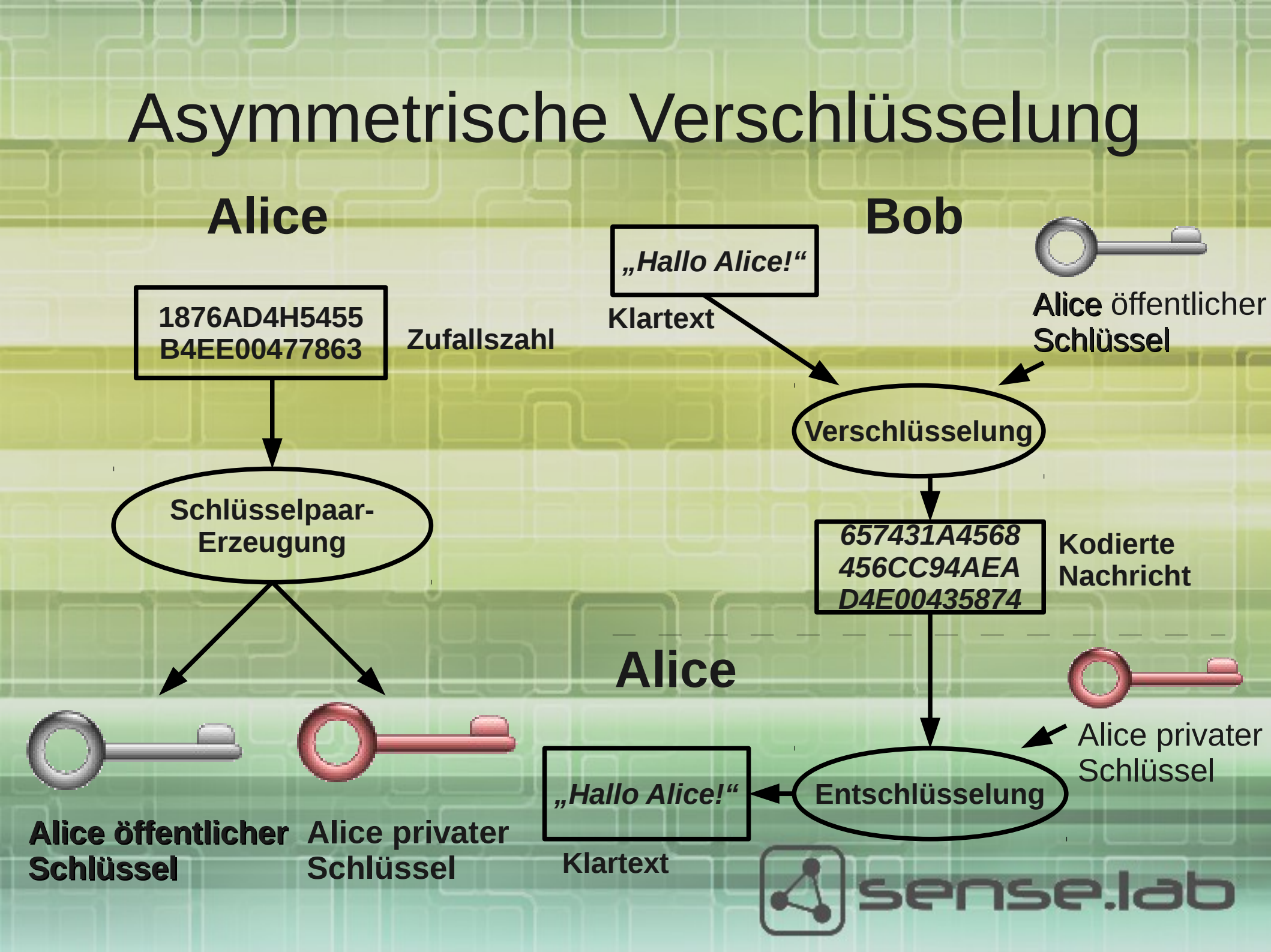
- technische Struktur
  - Netzwerk pot. unsicherer Knoten und Verbindungen
  - Knoten können von überall aus kontrolliert werden
- einfacher / risikoarmer Zugriff
  - alles Sys-Admins haben arbeitsbedingt Zugriff auf alle Daten
  - mitlesen, kopieren und Manipulation von Daten sind ohne Sicherheitsvorkehrungen nicht erkennbar
  - Zugriff aus dem Ausland sind i.d.R. rechtlich nicht sanktionierbar (falls es überhaupt zur Anzeige kommt)

Sicher kommunizieren in unsicheren Netzwerken?

- Asymmetrische Verschlüsselung -

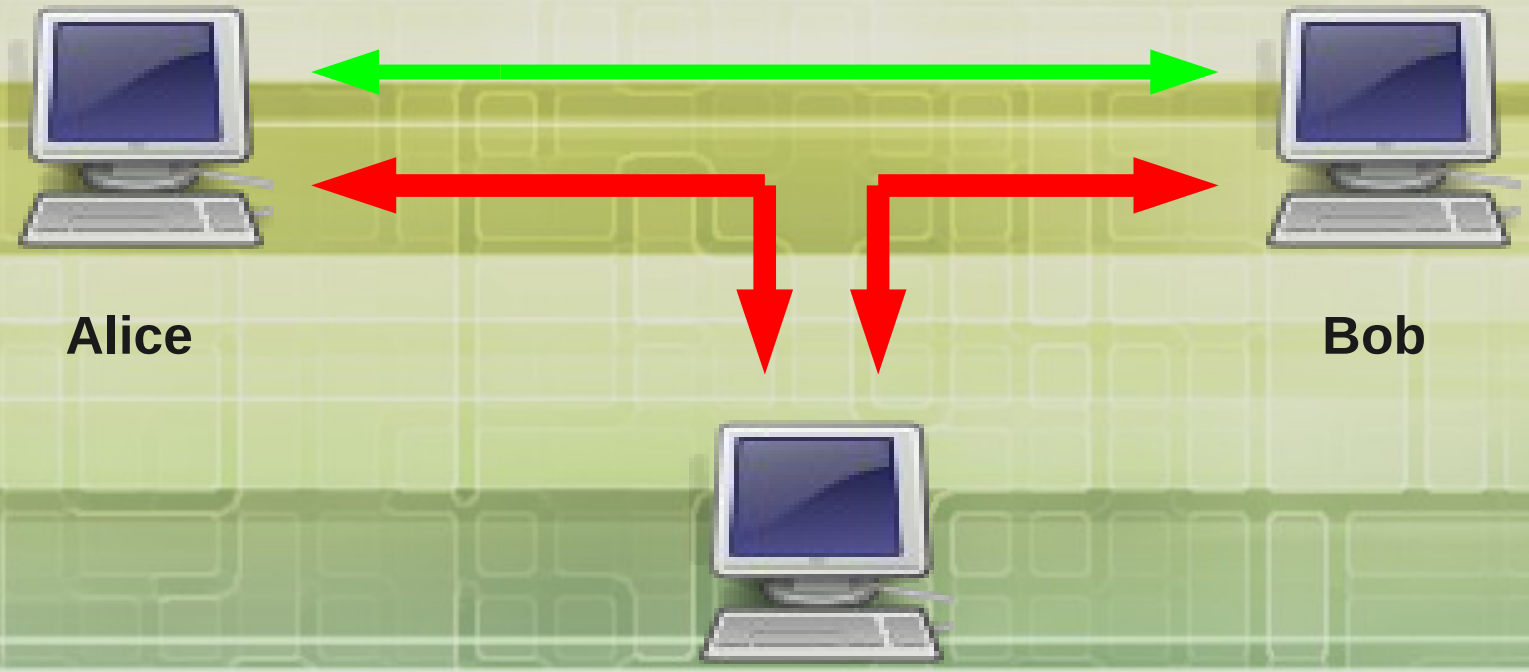
- gemeinsamer Schlüssel bei unsicheren Wegen nicht gefahrlos übermittelbar
- also ungleiche Schlüssel (trap-door-functions) für Ver- und Entschlüsselung
- öffentlicher Teil der Schlüssel (Verschlüsselung) kann gefahrlos über unsichere Verbindungen mitgeteilt werden
- Privater Teil des Schlüssel (Entschlüsseln) muß geheim gehalten werden

Asymmetrische Verschlüsselung



Wozu Fingerabdrücke?

- man in the middle attack -



direkte Verbindung

manipulierte Verbindung

sense.lab

Fingerabdrücke von Schlüsseln

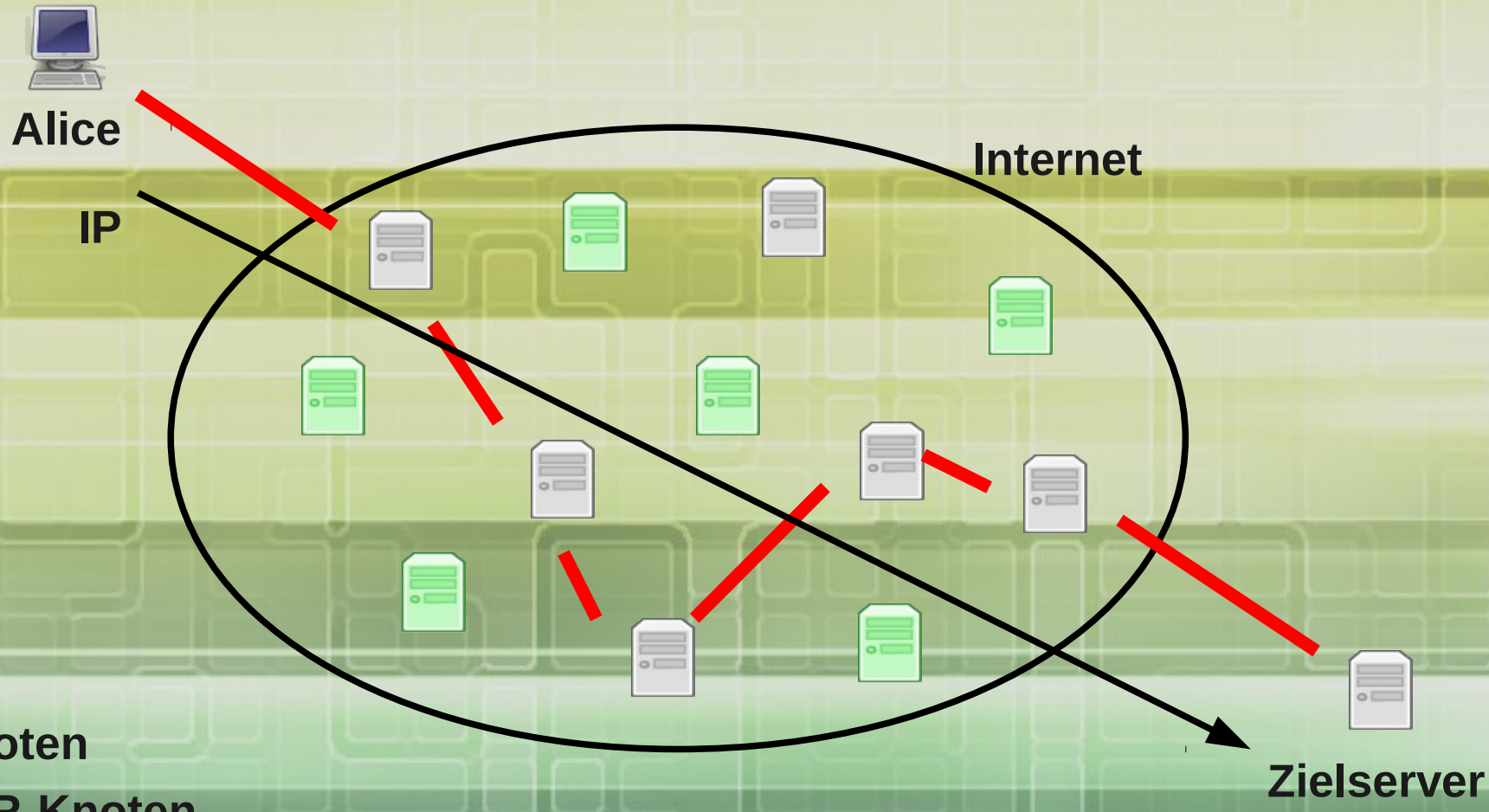
- jeder Datei lässt sich mit einer Rechenoperation eine Zahl zuordnen (=Fingerprint)
- ändert sich die Datei, ändert sich der Fingerprint
- wurden Dateien übermittelt, kann anhand des Fingerprints ermittelt werden, ob die Datei unterwegs sich verändert hat (Vgl. z.B. Telefon)

Sicheres Surfen im WWW

Onion-Routing mit TOR

sense.lab

Surfen



Knoten

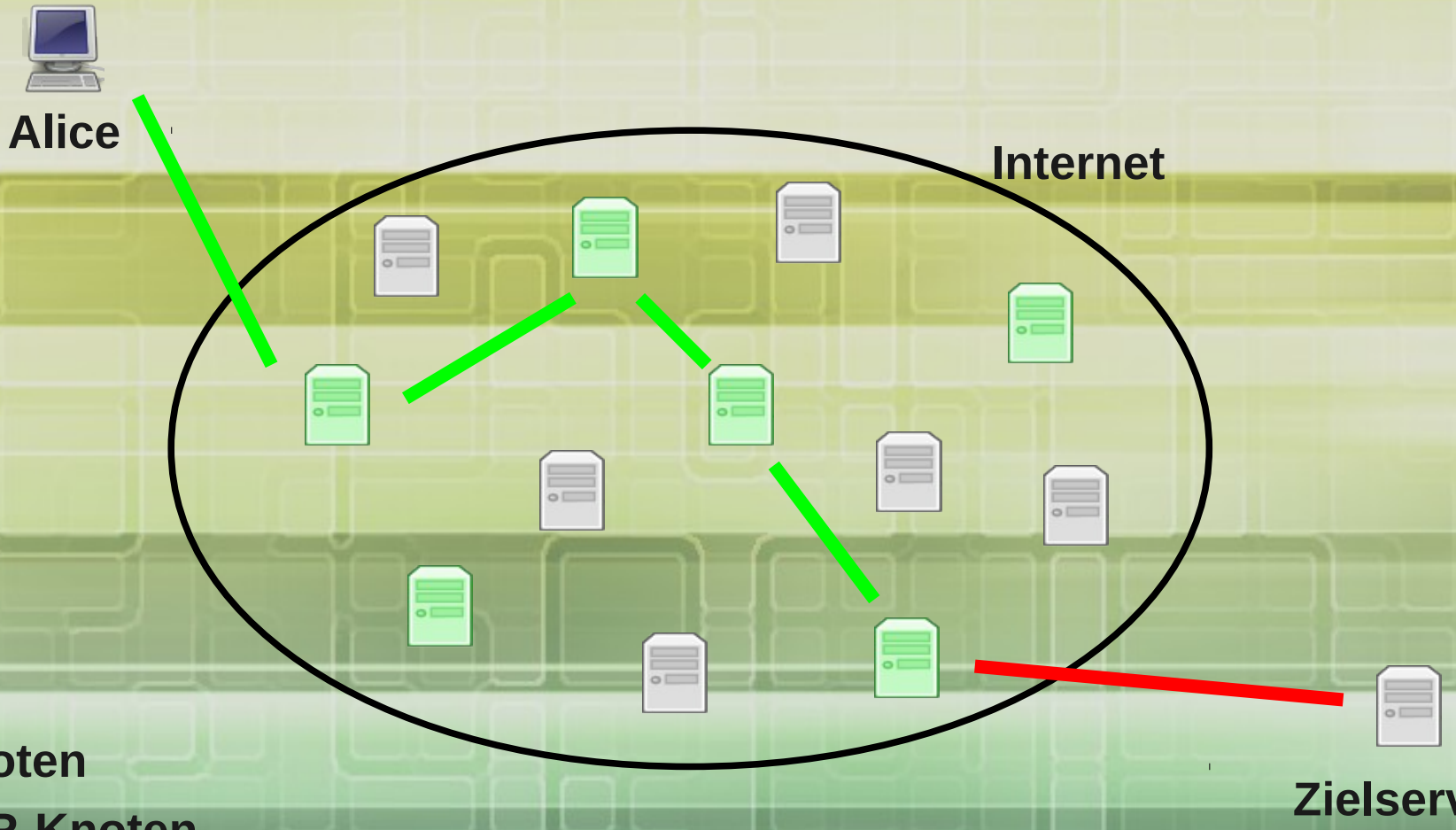
TOR-Knoten

verschlüsselte Verbindung

unverschlüsselte Verbindung

sense.lab

Anonymes Surfen mit TOR



Knoten

TOR-Knoten

verschlüsselte Verbindung

unverschlüsselte Verbindung

sense.lab