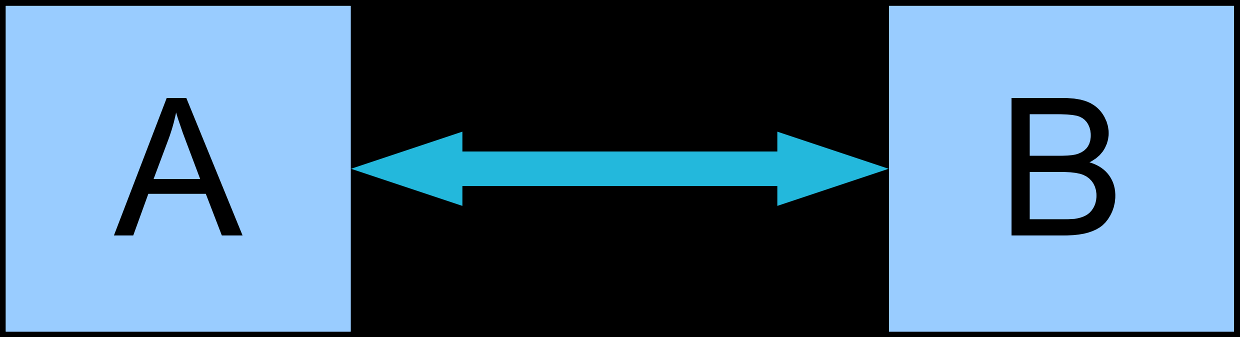
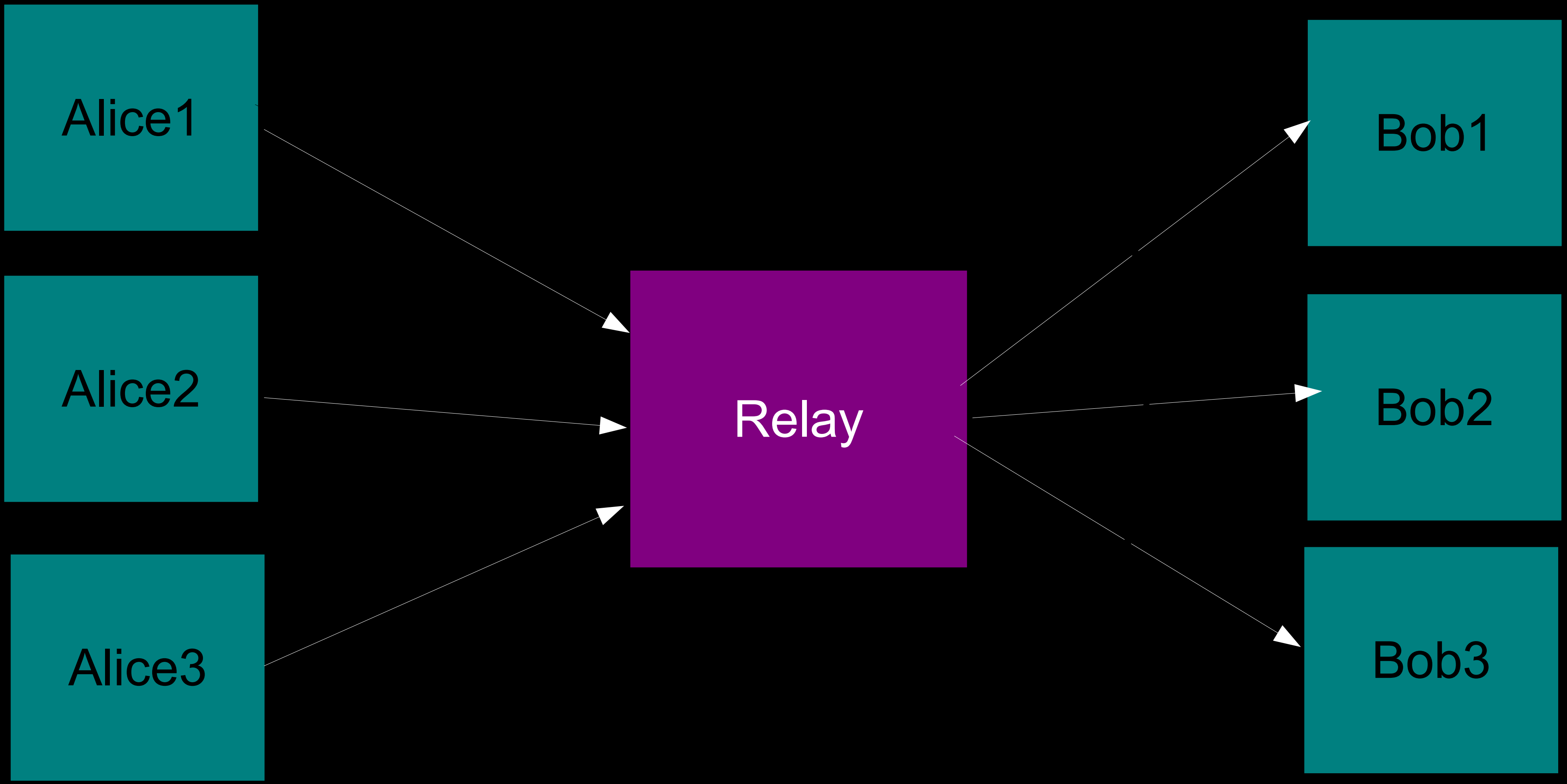
Anonymität?
Ünüberwachbare Kommunikation!



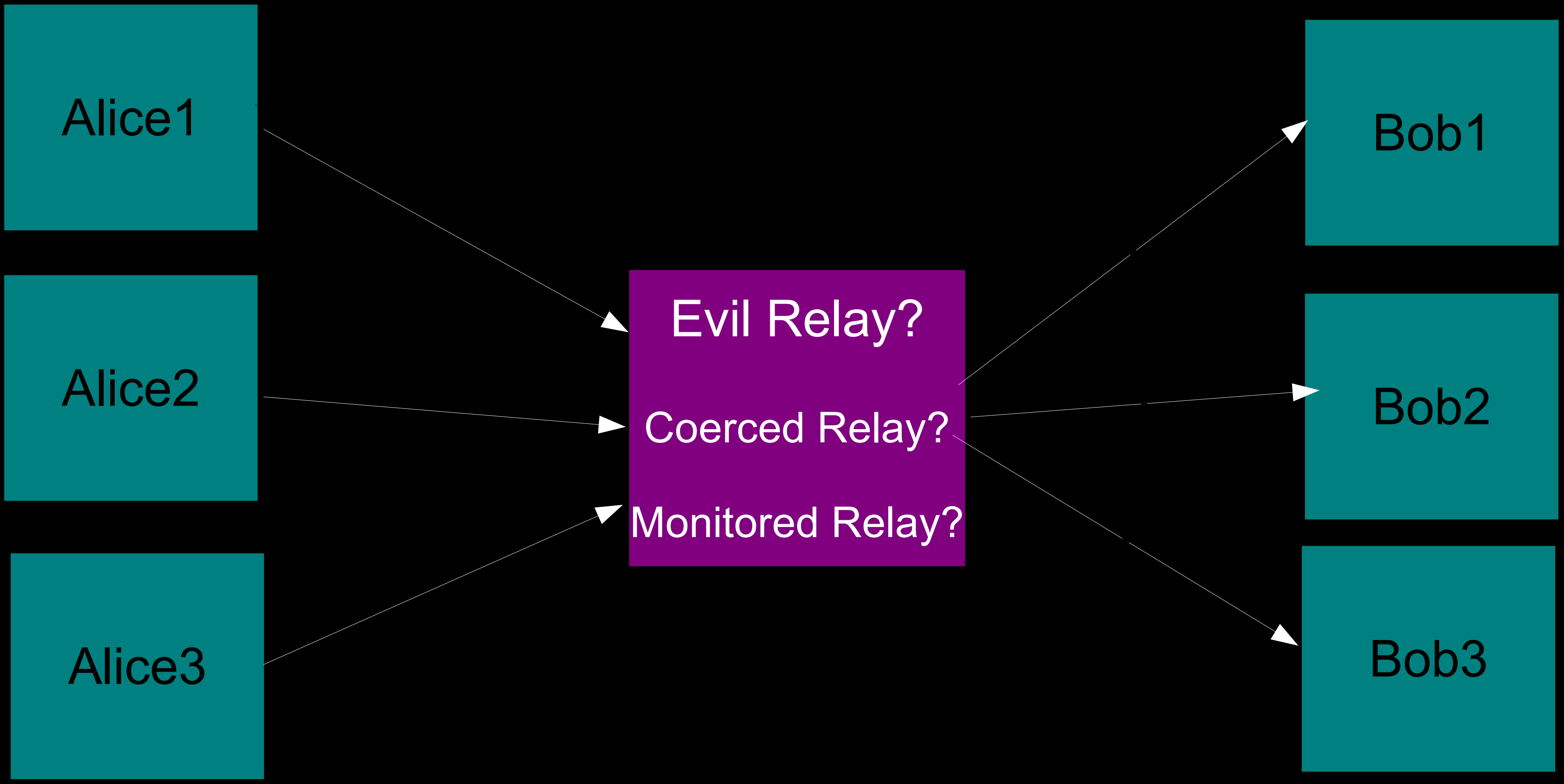
Verschlüsselung schützt nur Inhalte, nicht die Metadaten!

- Wer mit wem?
- Wann?
- ~~Was?~~

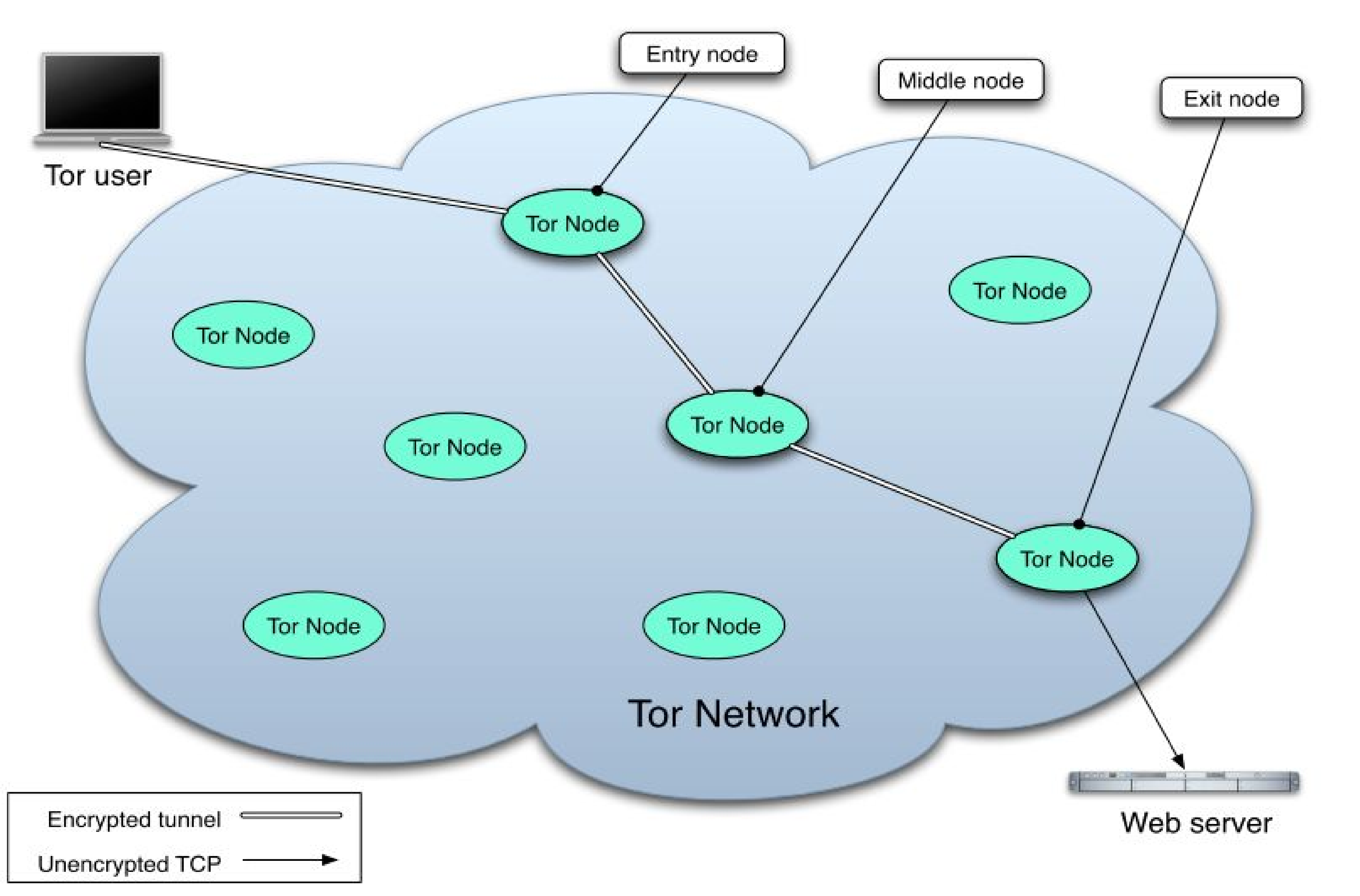
1-hop proxy (VPN, SSH Tunnel etc)



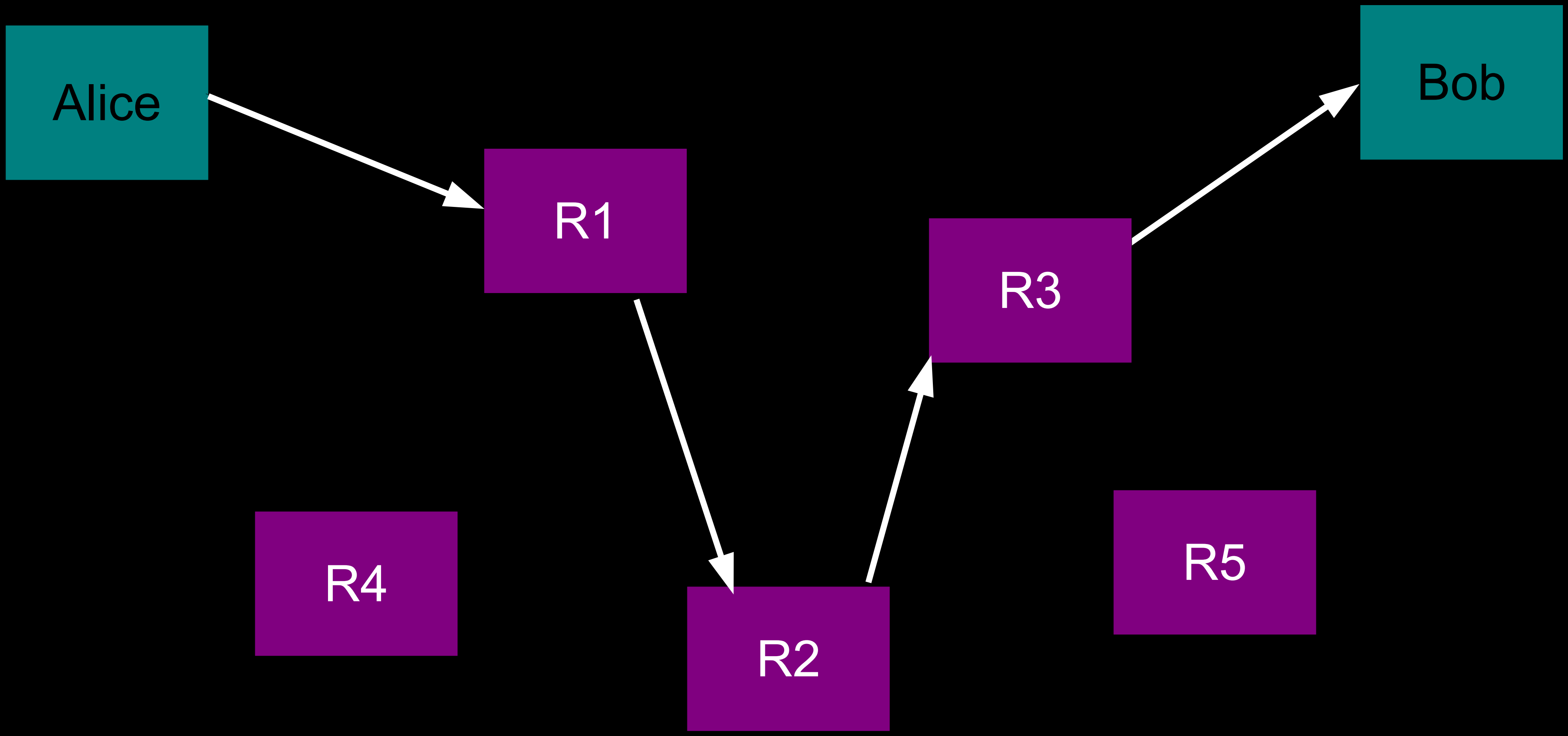
Problem Vertrauenswürdigkeit und einfache Überwachbarkeit



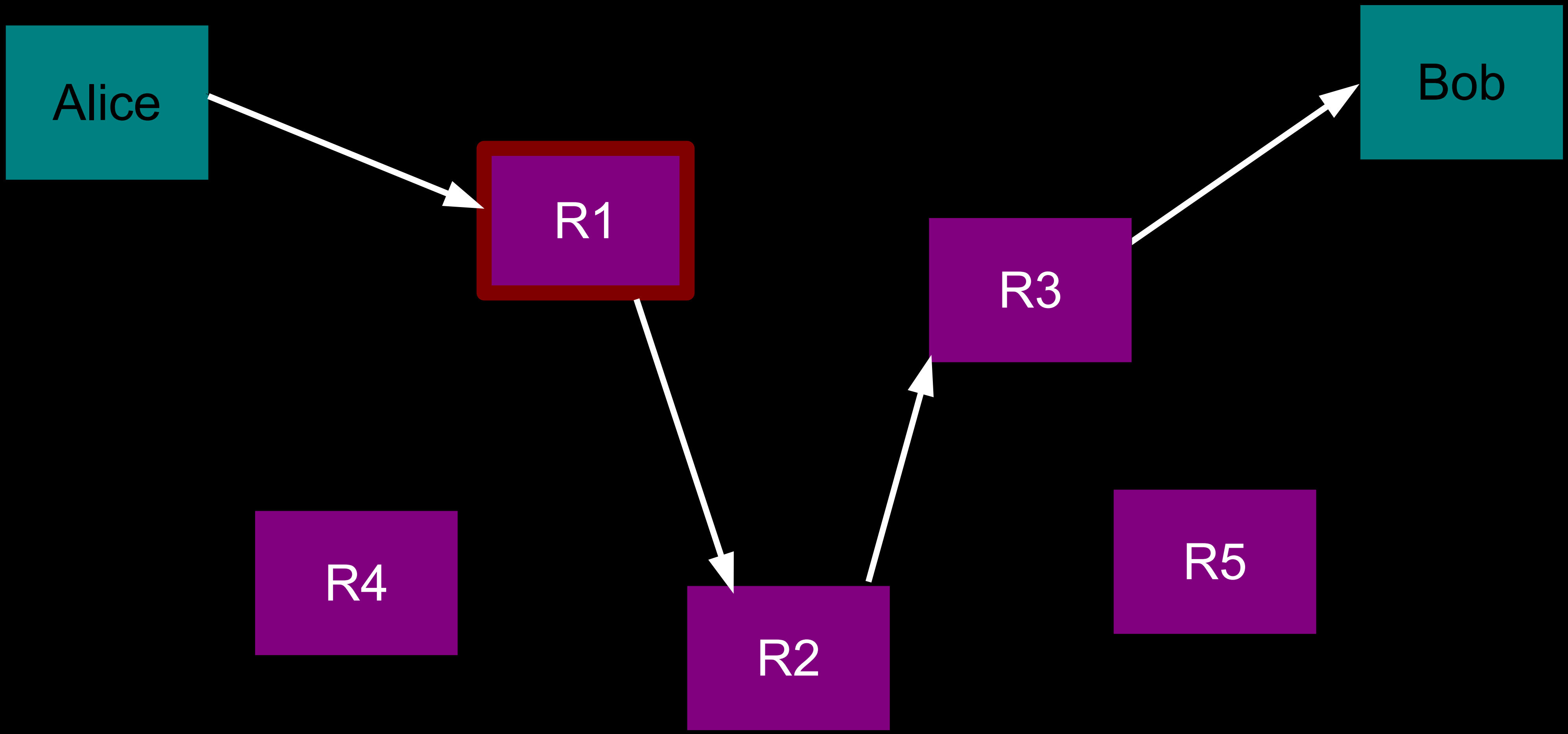
Tor


Entry node
Middle node
Exit node
Tor user
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Network
Web server
Encrypted tunnel
Unencrypted TCP

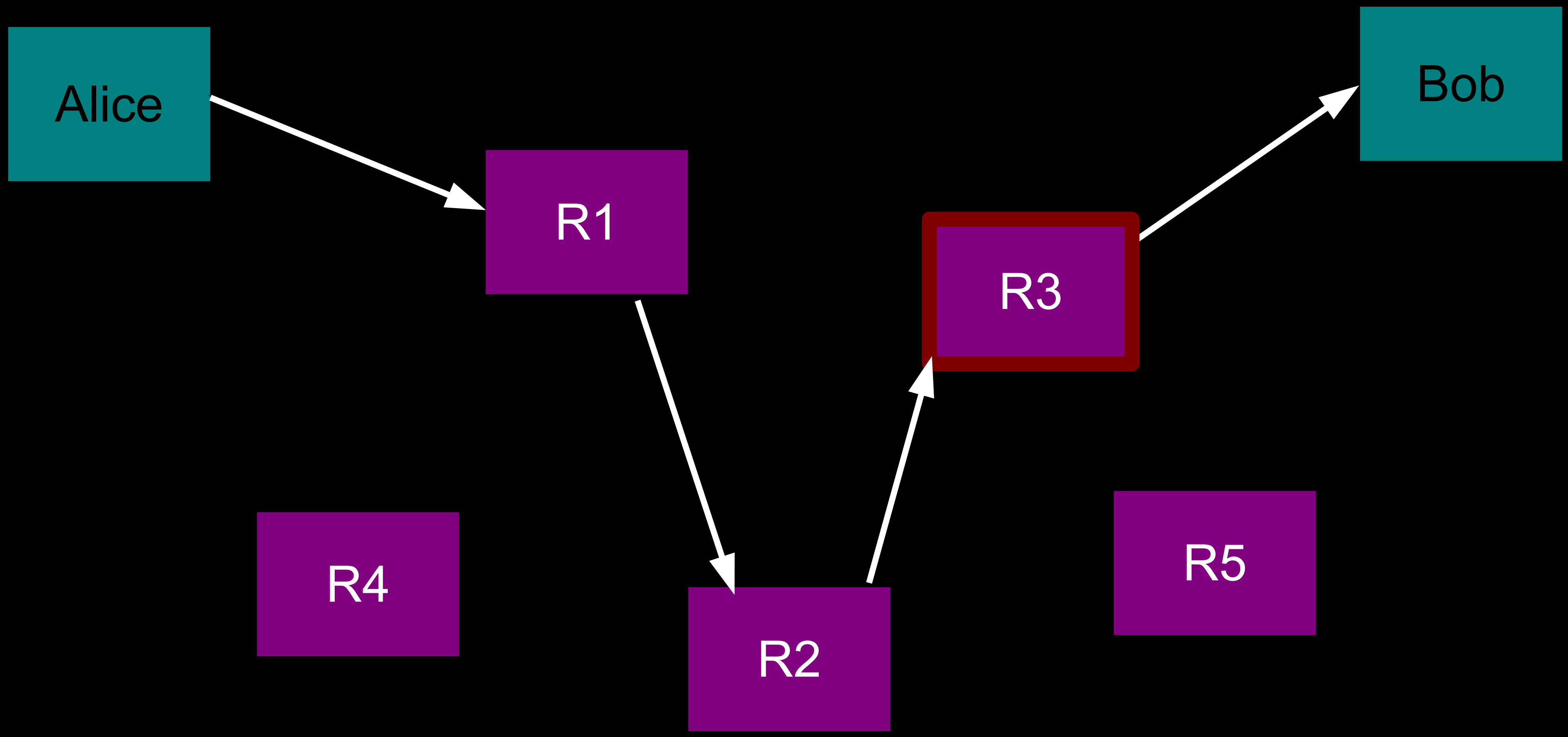
Tor



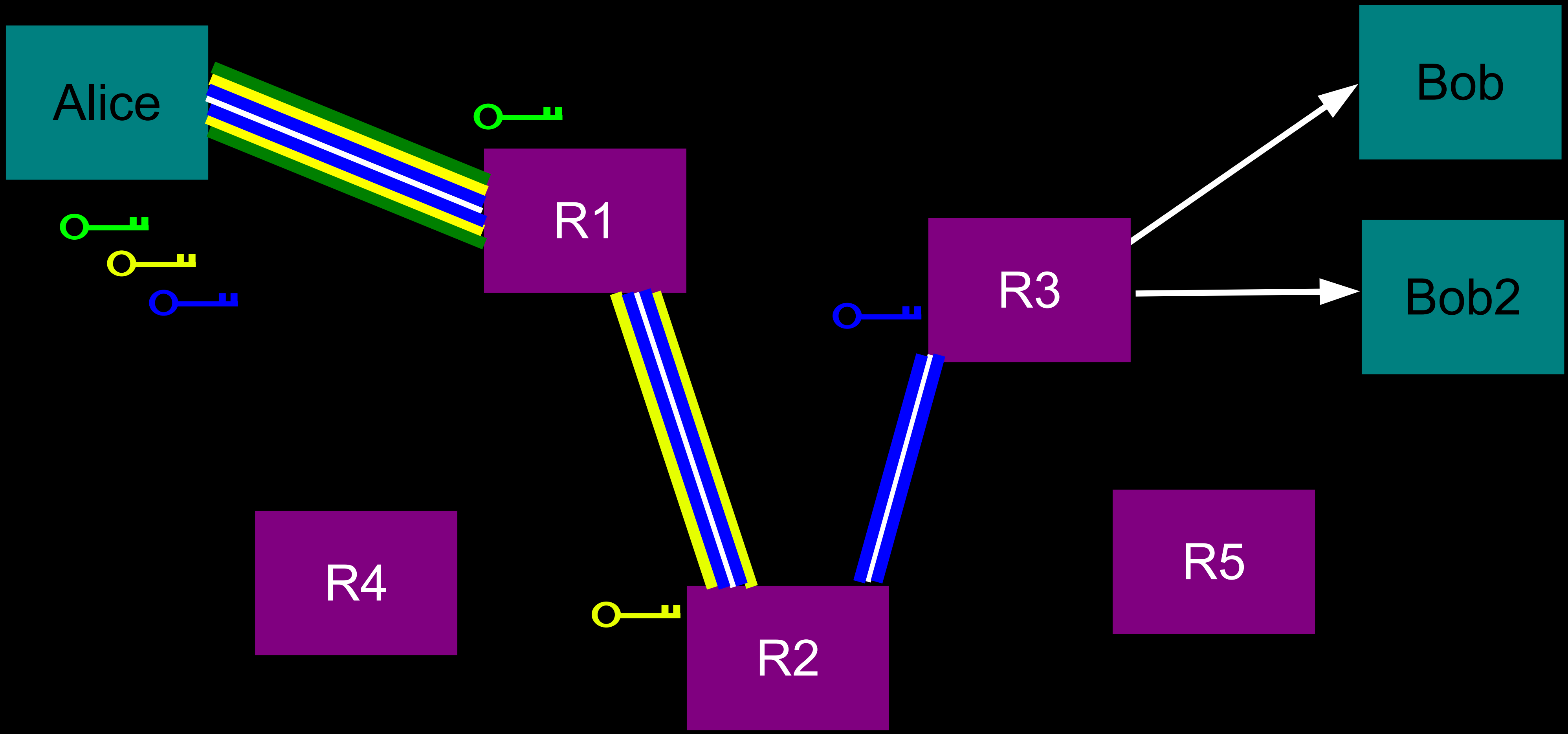
Tor



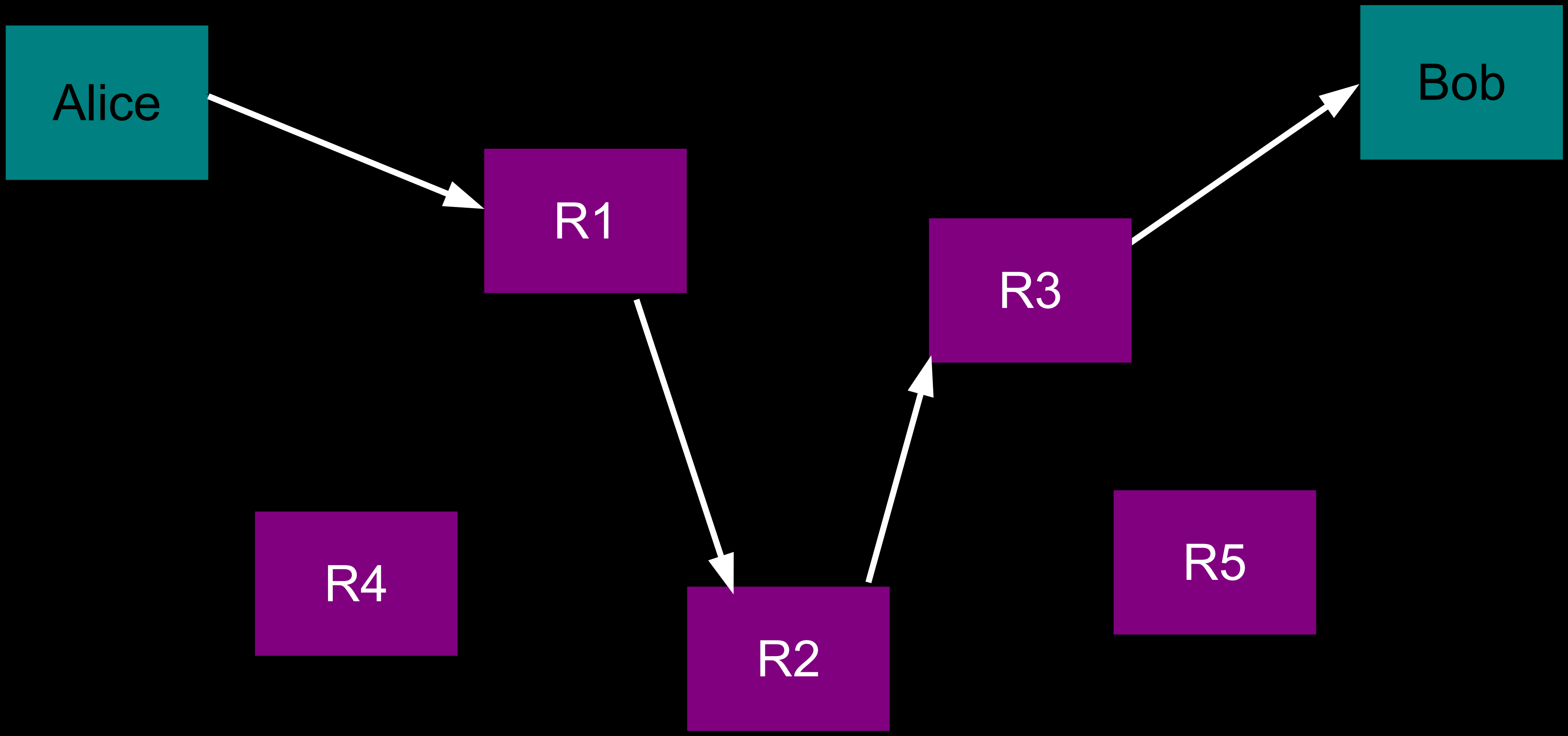
Tor



Tor



Problem: (sufficiently) global passive adversaries

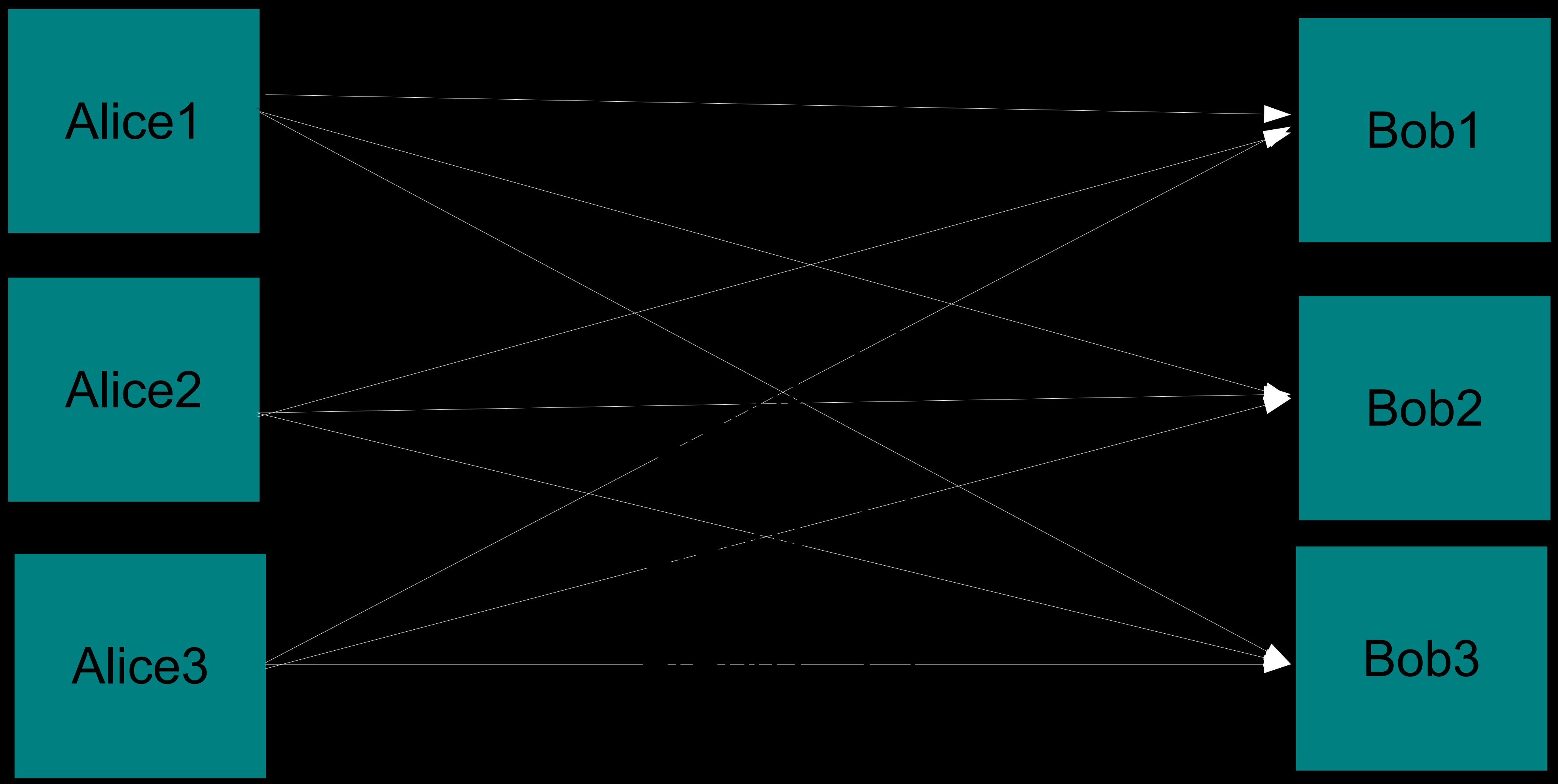


- “Not secure against end-to-end attacks: Tor does not claim to completely solve end-to-end timing or intersection attacks.“ (Tor Design Paper, 2004)
- A global passive adversary is the most commonly assumed threat when analyzing theoretical anonymity designs. **But like all practical low-latency systems, Tor does not protect against such a strong adversary.**“ (ebd.)

"The results show that Tor faces even greater risks from traffic correlation than previous studies suggested. An adversary that provides no more bandwidth than some volunteers do today can deanonymize any given user within three months of regular Tor use with over 50% probability and within six months with over 80% probability."

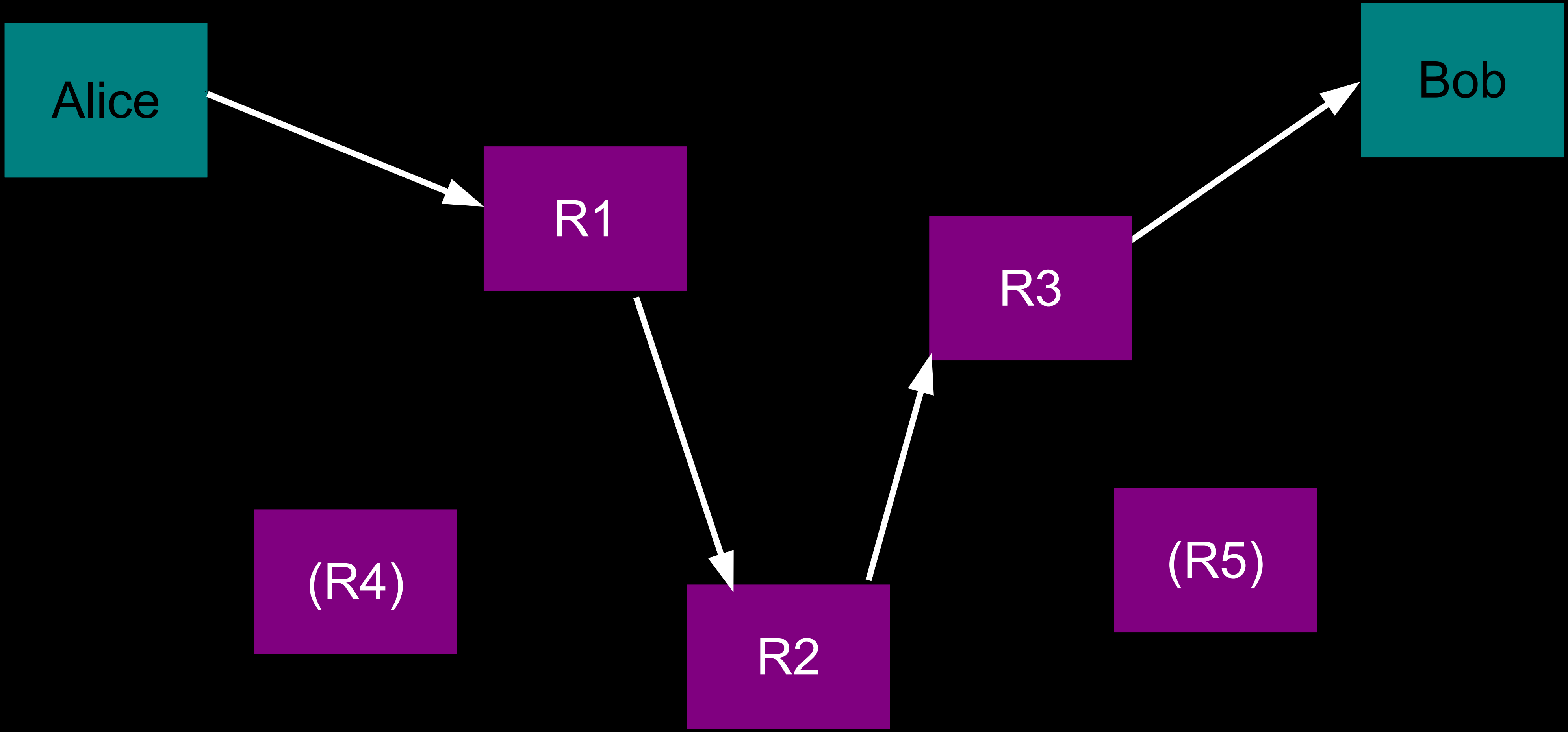
(Users get routed: Traffic Correlation on Tor by Realistic Adversaries, 2013)

Alternative: Broadcast-Architektur

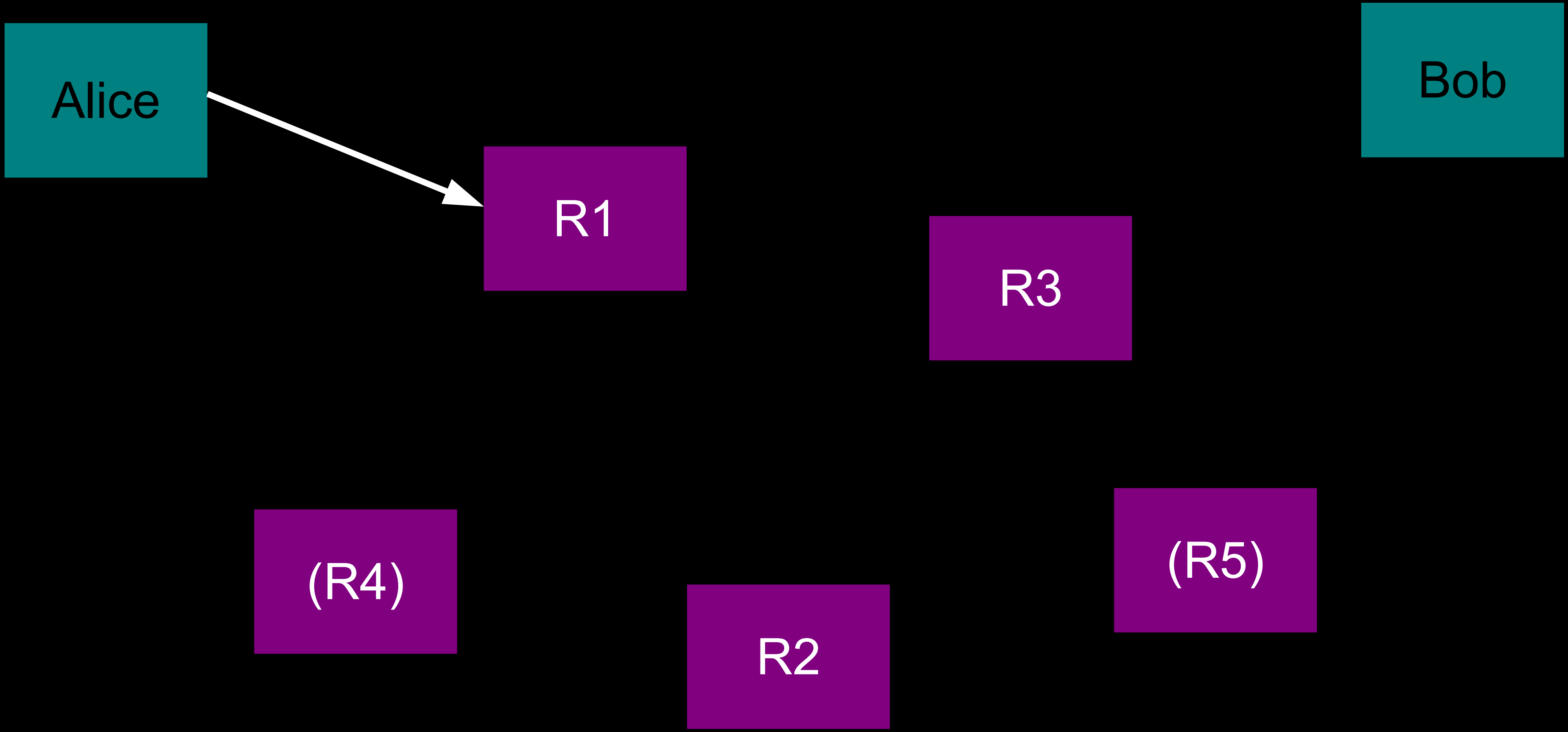


Beispiel Bitmessage

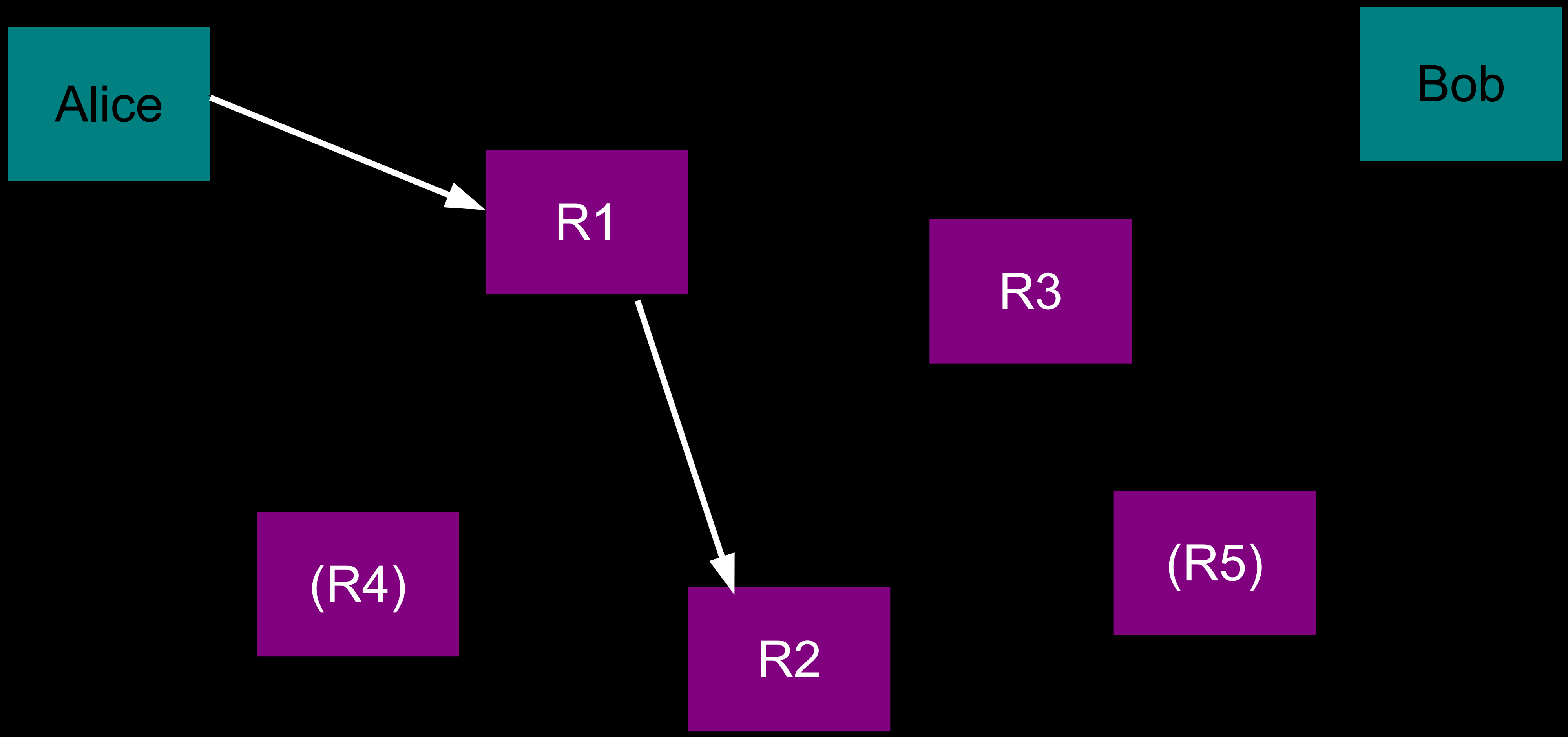
Alternative: Mixnets



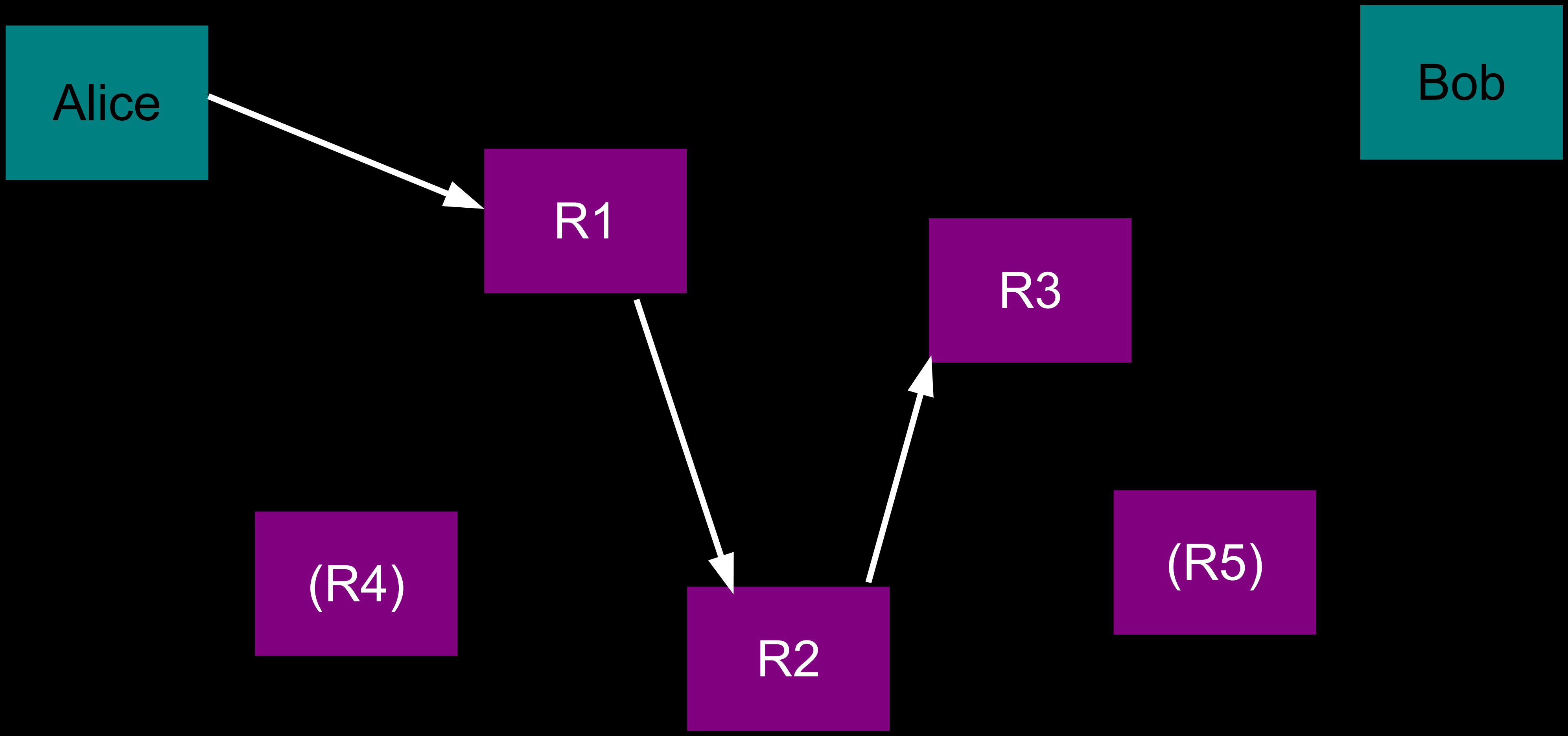
Tor: Verbindungsaufbau



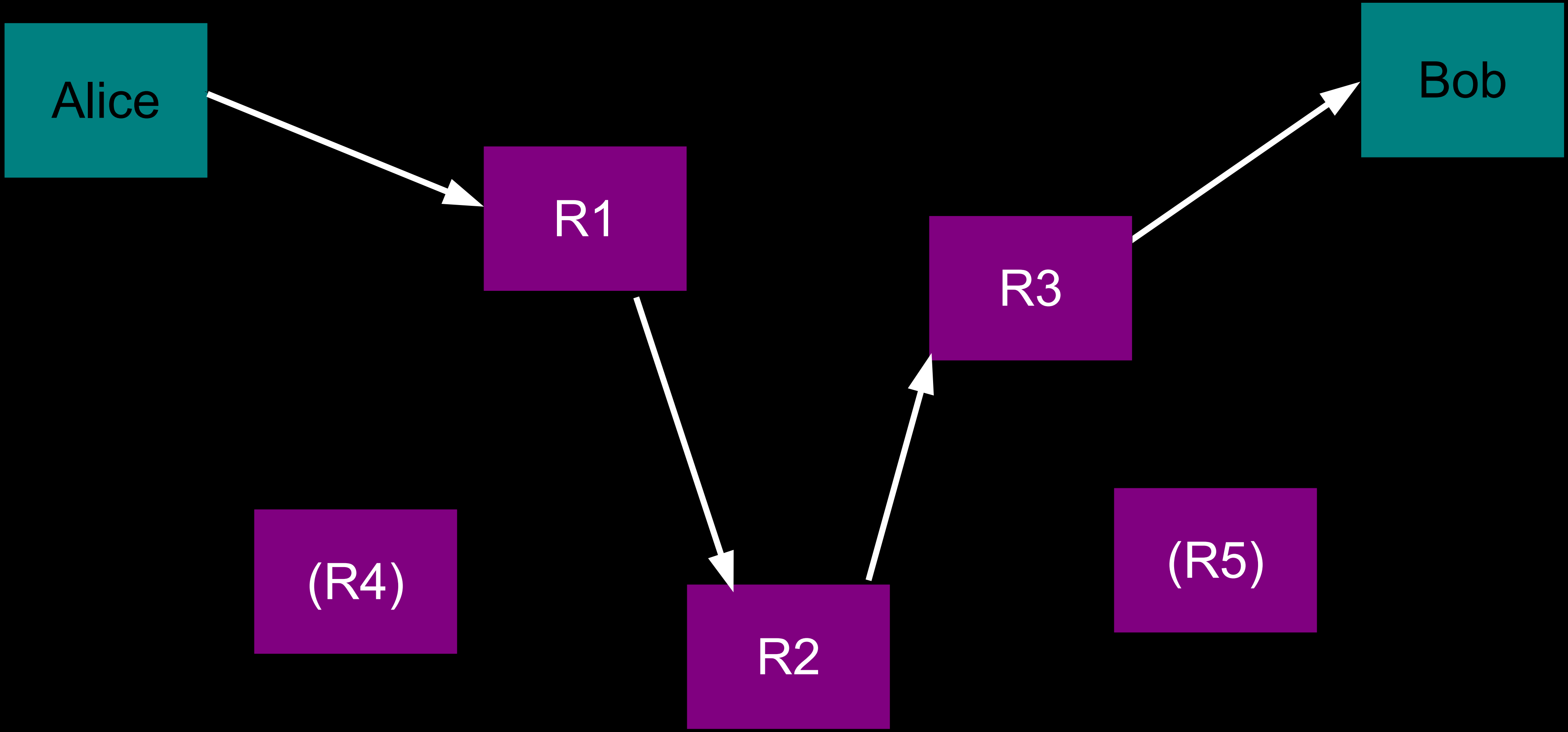
Tor: Verbindungsaufbau



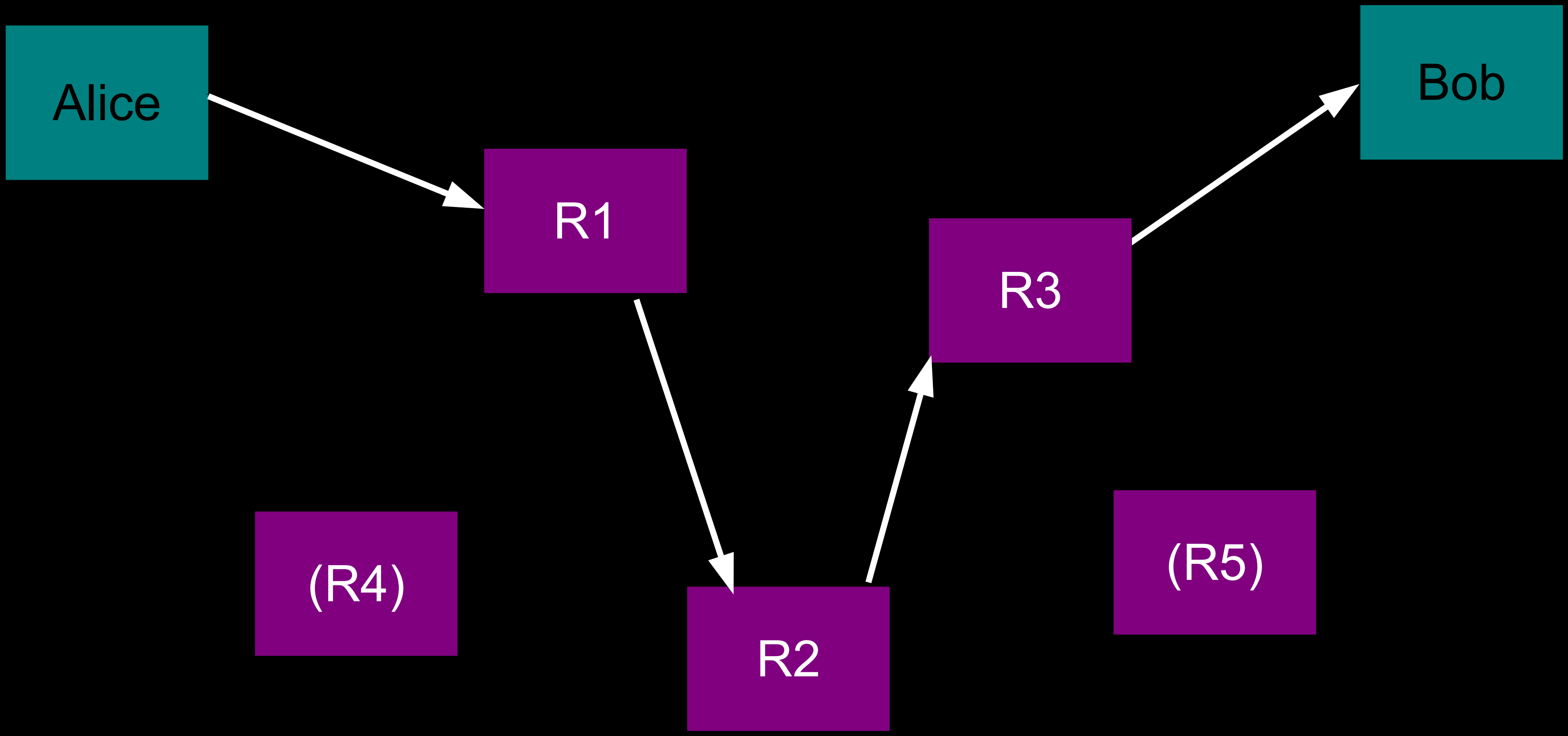
Tor: Verbindungsaufbau

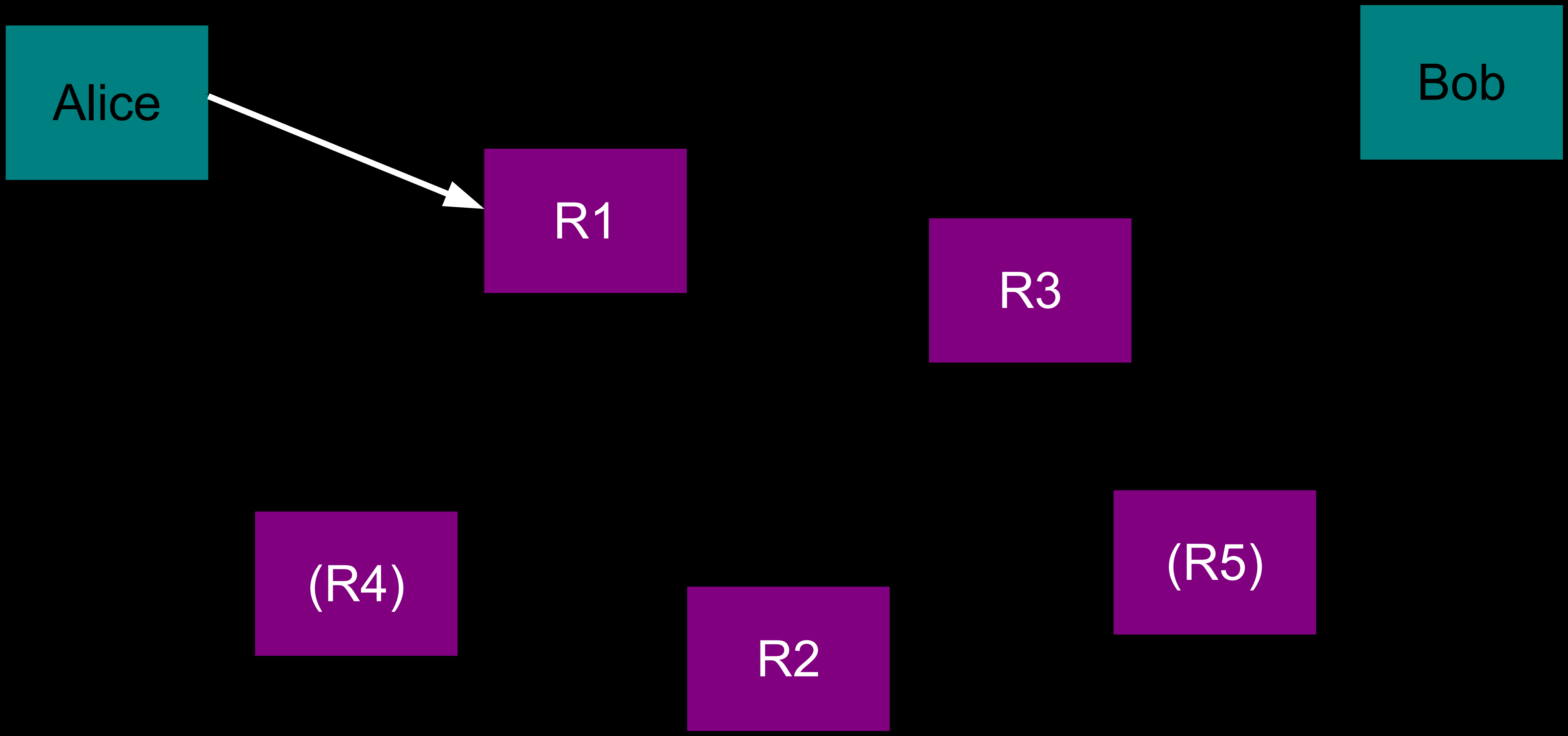


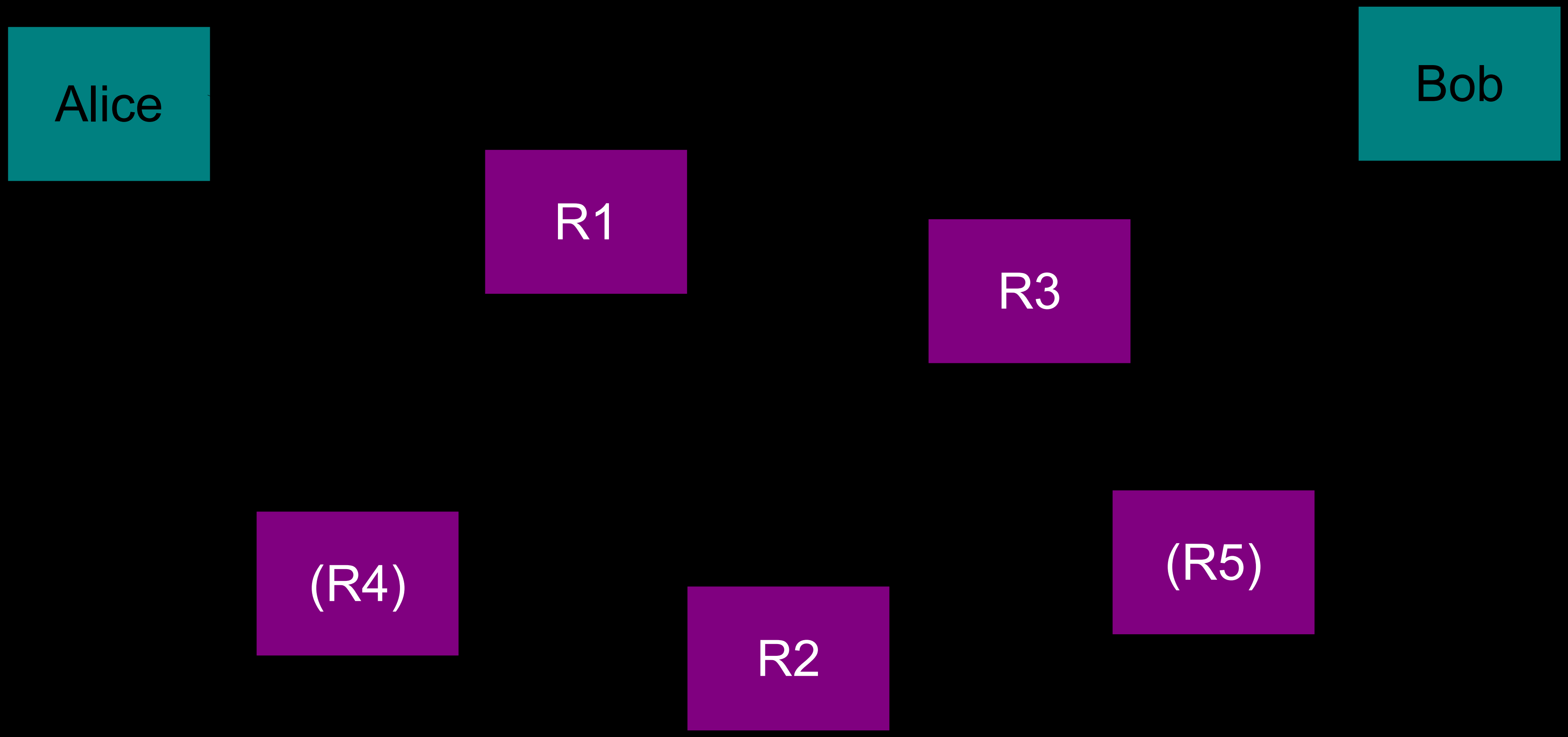
Tor: Verbindungsaufbau

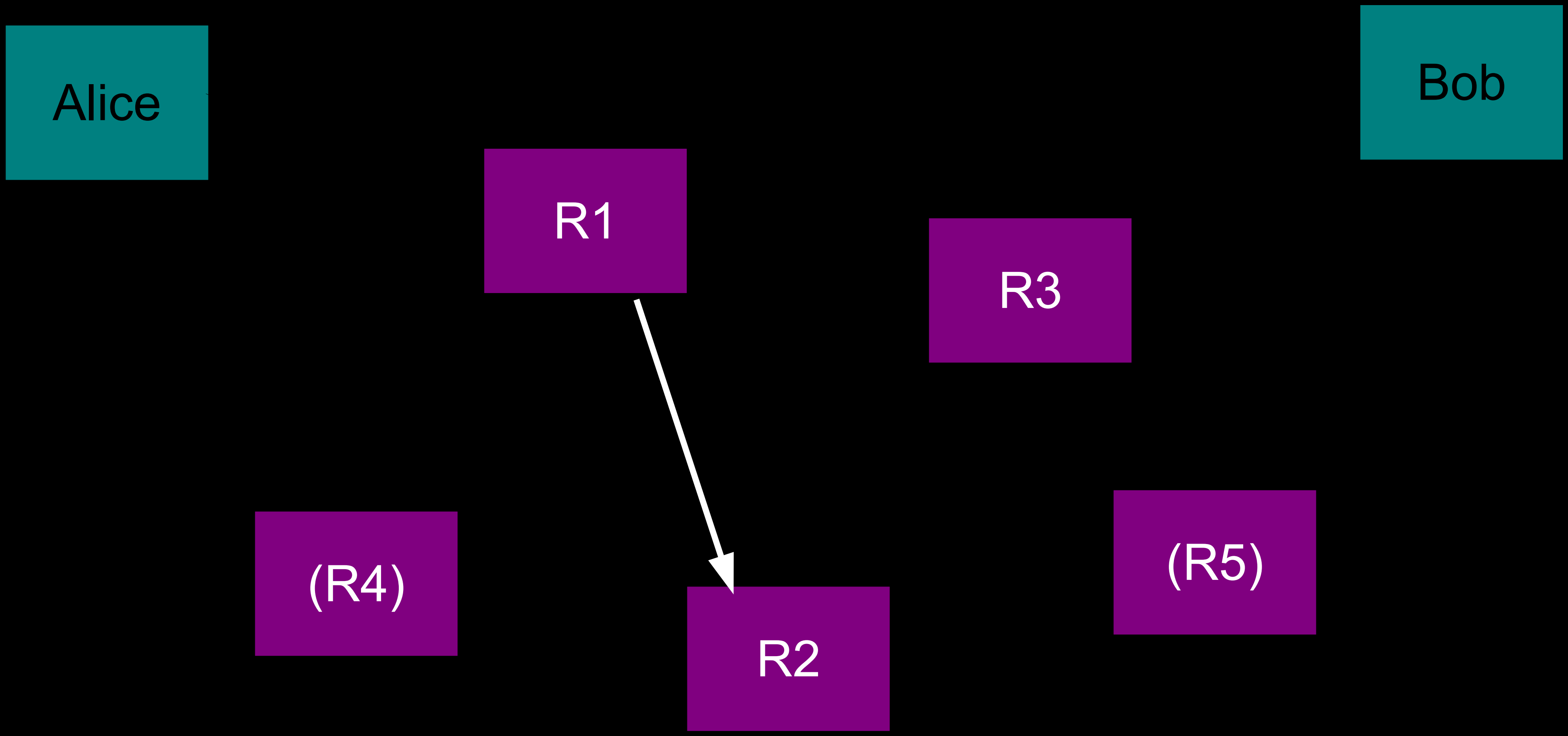


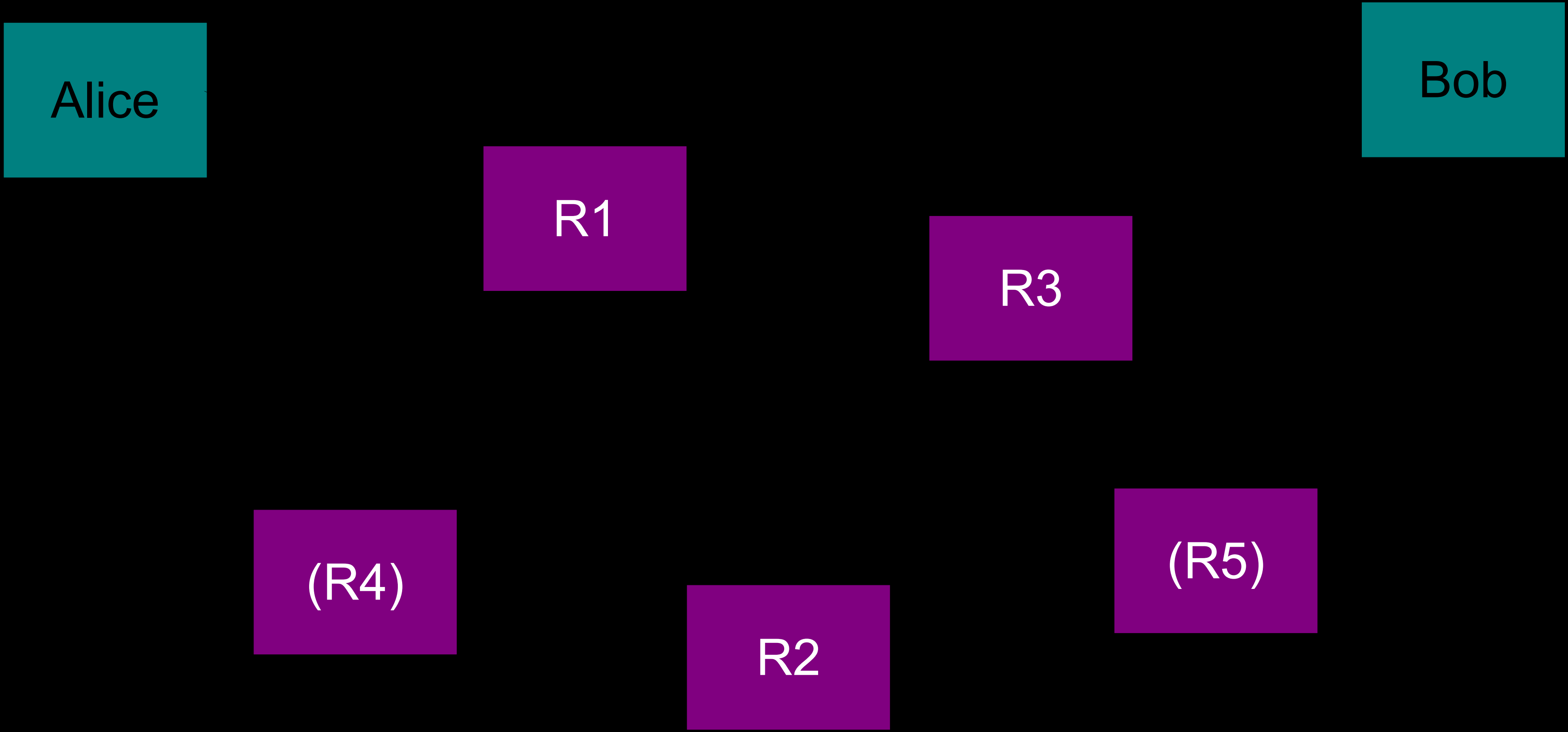
Mixnets: nachrichtenbasiert statt paketbasiert !

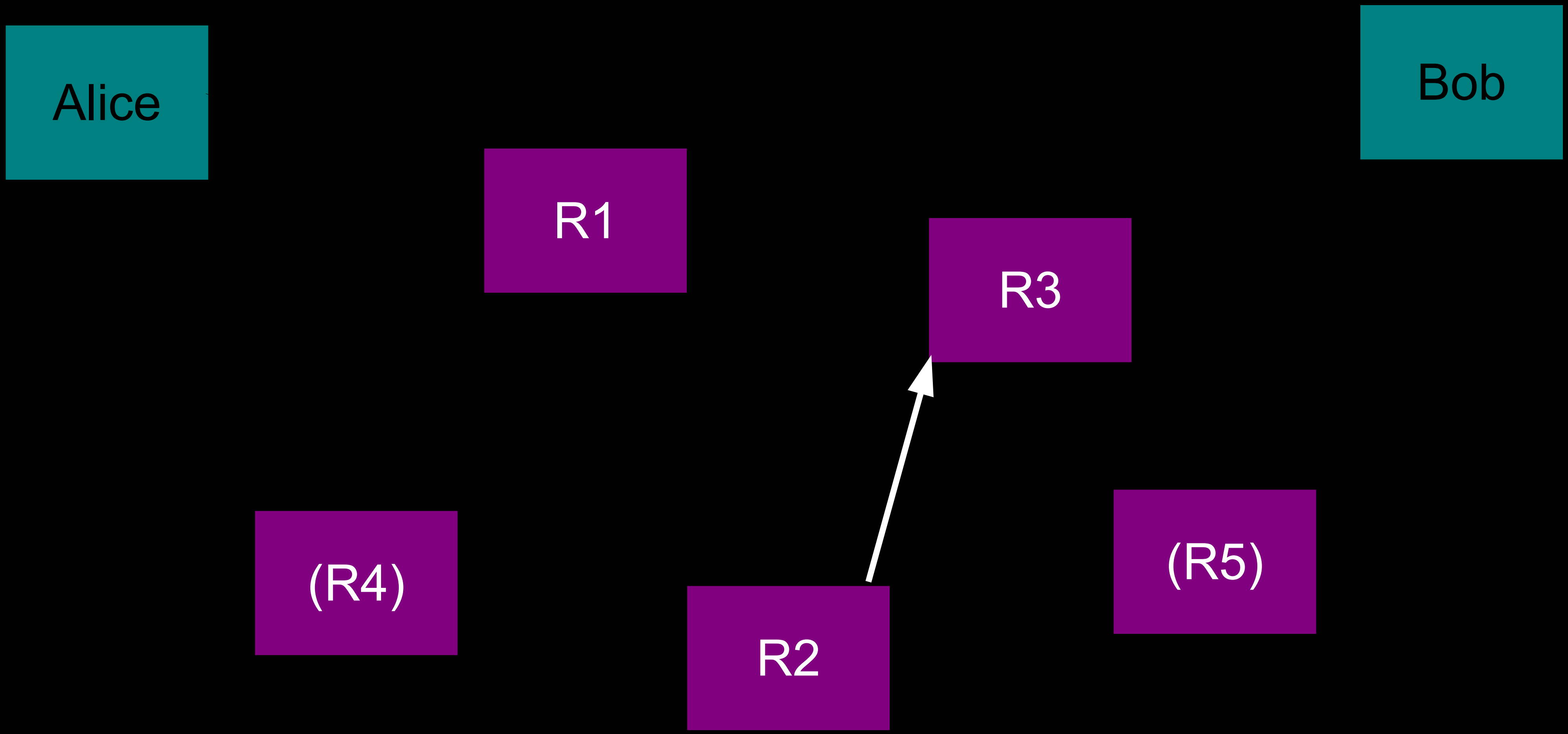


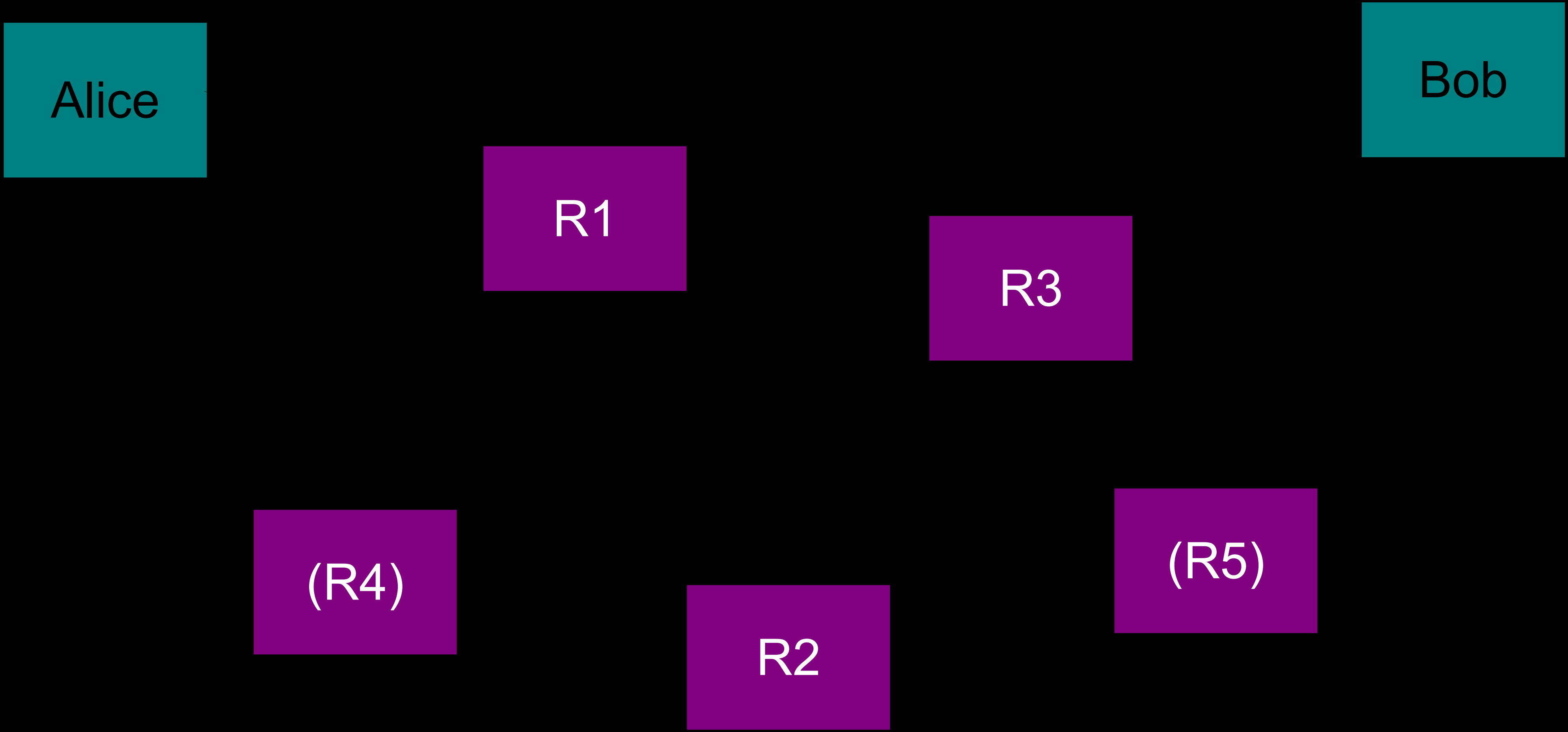

Alice
Bob
R1
R3
(R4)
(R5)
R2

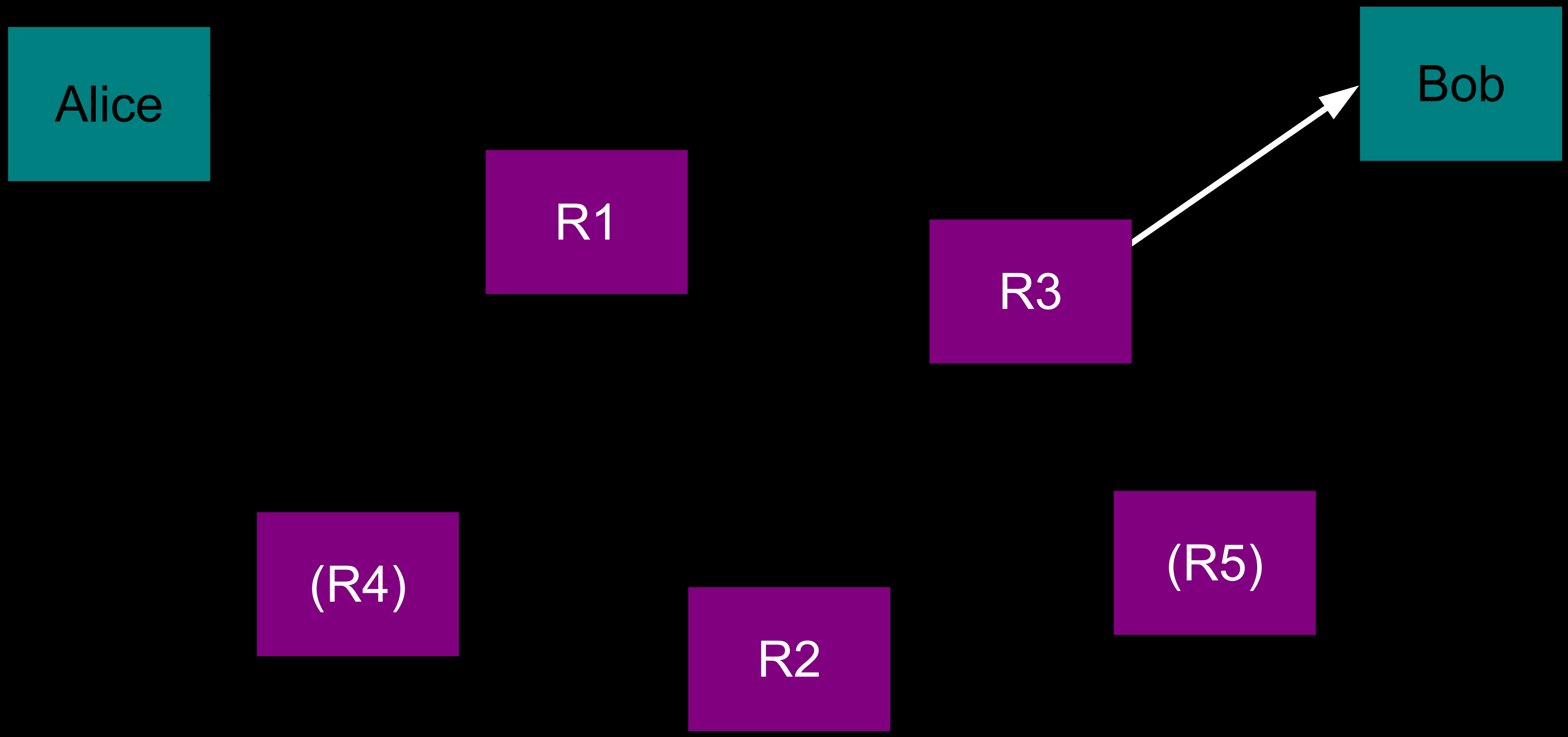

Alice
Bob
R1
R3
(R4)
(R5)
R2


Alice
Bob
R1
R3
(R4)
R2
(R5)

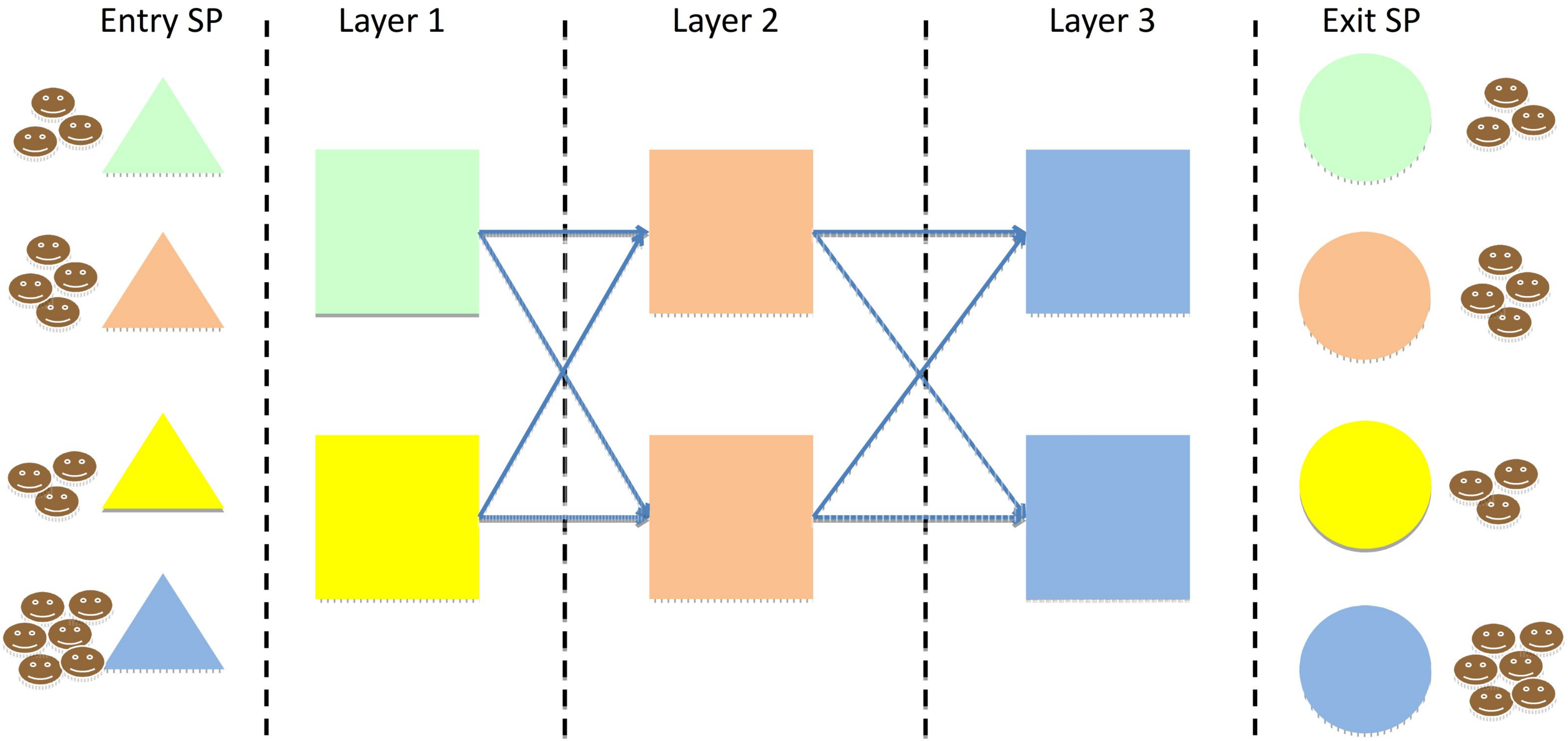

Alice
Bob
R1
R3
(R4)
R2
(R5)


Alice
Bob
R1
R3
(R4)
R2
(R5)


Alice
Bob
R1
R3
(R4)
(R5)
R2


Alice
Bob
R1
R3
(R4)
(R5)
R2

Mixnet Architecture



Colour: realms of trust (same SP)

Mix-Strategien

- Pool/Batching Mix
    - sammle x Nachrichten (“threshold mix”)
    - warte x Minuten (“timed mix”)

  (Mixmaster: timed + threshold: nur wenn x Nachrichten eingangen sind wird Queue nach Timeout geleert/versendet)

- Stop & Go Mixes: Delay der einzelnen Hops vom Nutzer vorgegeben

- 1978 Limitations of End-to-End Encryption in Secure Computer Networks (Karger)
- 1981 Untraceable electronic mail, return addresses and digital pseudonyms (David Chaum)
- 1985 Networks Without User Observability – Design Options (Pfitzmann)
- 1991 ISDN-Mixes (Pfitzmann)
- [1995 "Initial work on Onion Routing begins"]
- 1998 Real-Time MIXes (Pfitzmann)

http://freehaven.net/anonbib

- 1992 anon.penet.fi (Typ 0 Remailer)

  (500,000 Nutzer, 8000 Nachrichten/Tag, ~$1000/Monat) [1]

  1995: Church of Scientology, Los Angeles → FBI → Finnland

- 1992 Cypherpunks-Remailer (Typ 1 Remailer)

  Einfacher Remailer, kein Mixing (→ timing analysis), kein Padding (→ traffic analysis)

- 1994 Mixmaster (Typ 2)
- 1995 anonymizer, c2.net nymserver
- 2002 Mixminion (Typ 3)
- [2004 Tor Design Paper]

[1] http://freehaven.net/anonbib/cache/remailer-history.html

Probleme Mixnets

- Historisch:
  - Keine Zustellungsgarantie
  - Lange Nachrichtenlaufzeiten (Tage!)
  - Komplizierte UIs, fehlende Integration
  - Spam-/Abuse-Problematik
- Loopix Anonymity System (März 2017)
  - Stop & Go
  - aktive Angriffe erkennen durch “loops”
  - “message latency in the order of seconds”

Katzenpost

- “echtes” Open Source Projekt
  - Spezifikation auf Github
  - Implementierung in Go
  - [Integration in K9 Mail]
  - Finanzierung durch EU!

https://katzenpost.mixnetworks.org/