Anonymität nach Tor

moritz bartl

moritz@torproject.org
PGP: FAFF CBB0 BB9E 4410 6A51 BBA0 ECE9 21DA 863B 95F7

Have you seen
this dog?

I have now
I have now
I have now
I have now
I have now
I have now
I have now

2004

2010

Stiftung

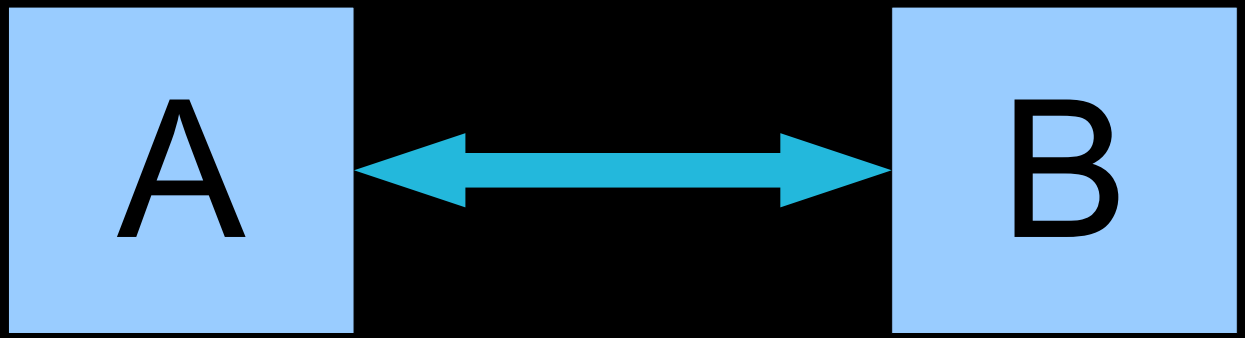
Erneuerbare Freiheit

2013

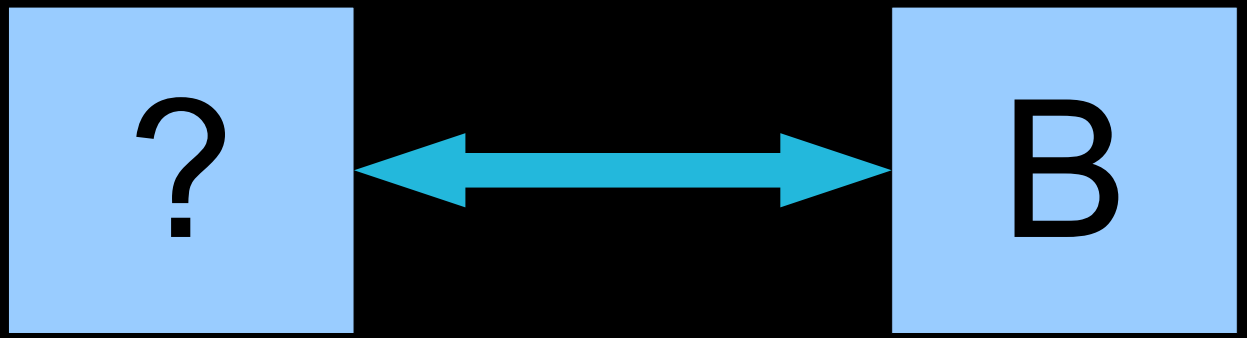
Center for the Cultivation of Technology

2016

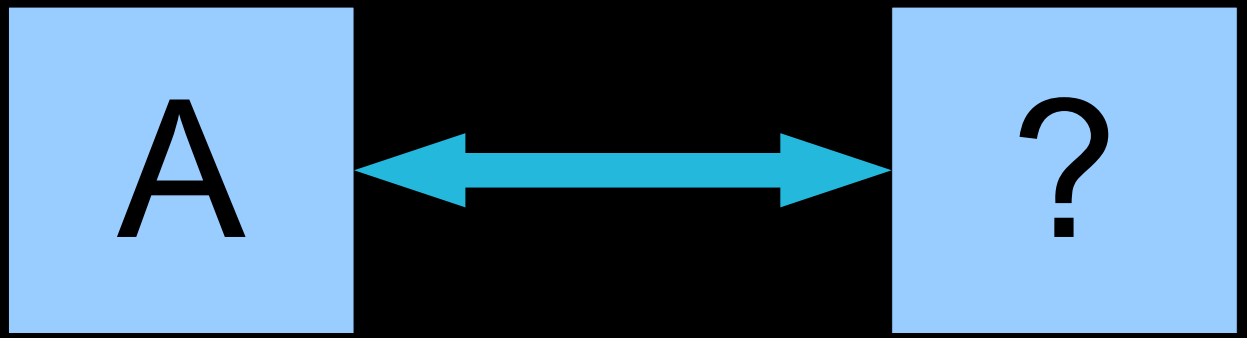
Anonymität?



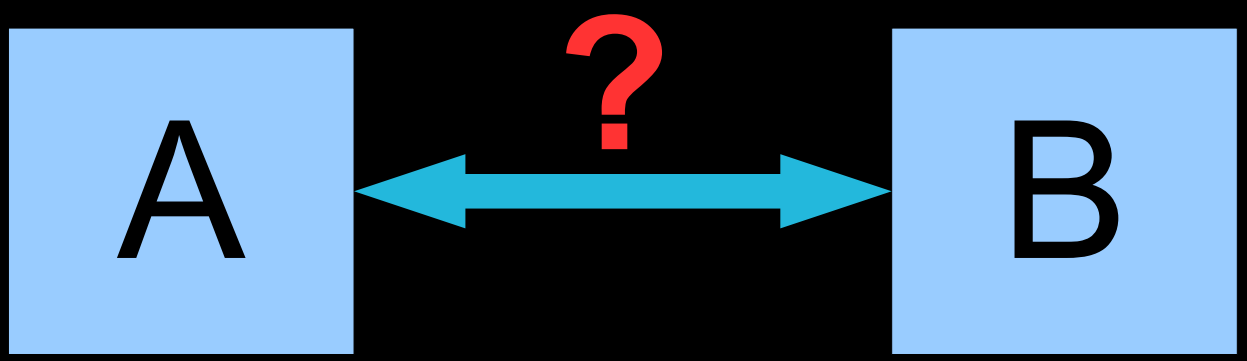
Senderanonymität



Empfängeranonymität

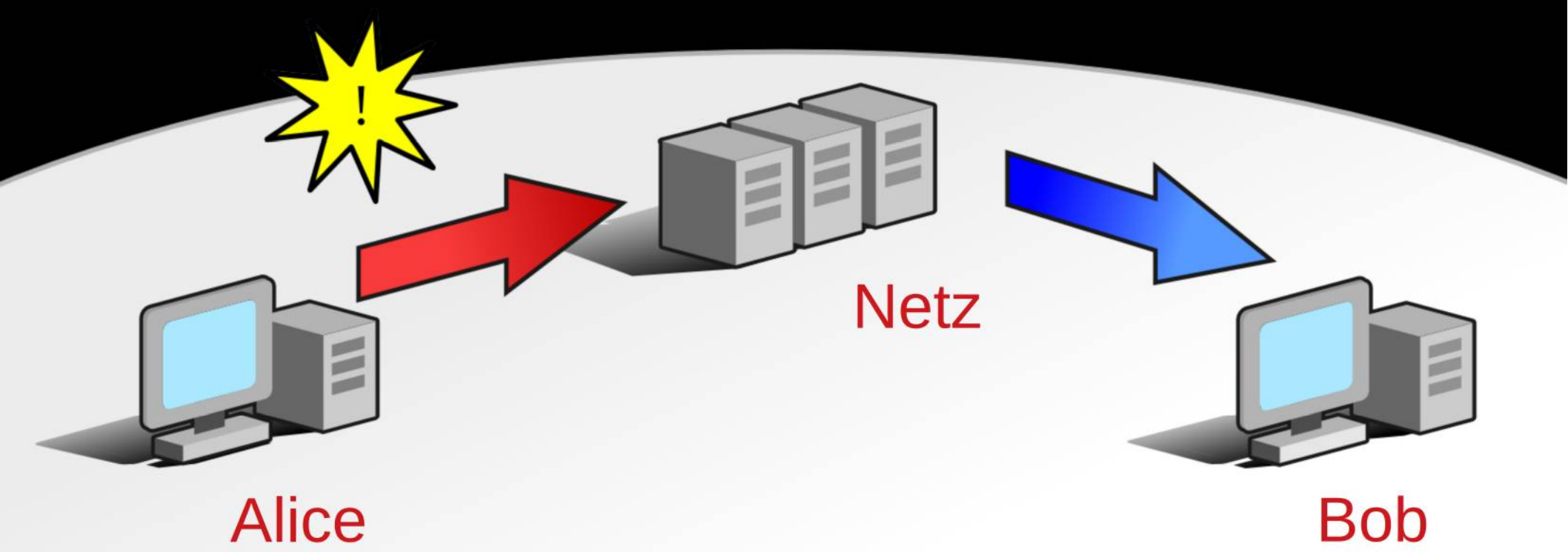


Anonyme Kommunikation

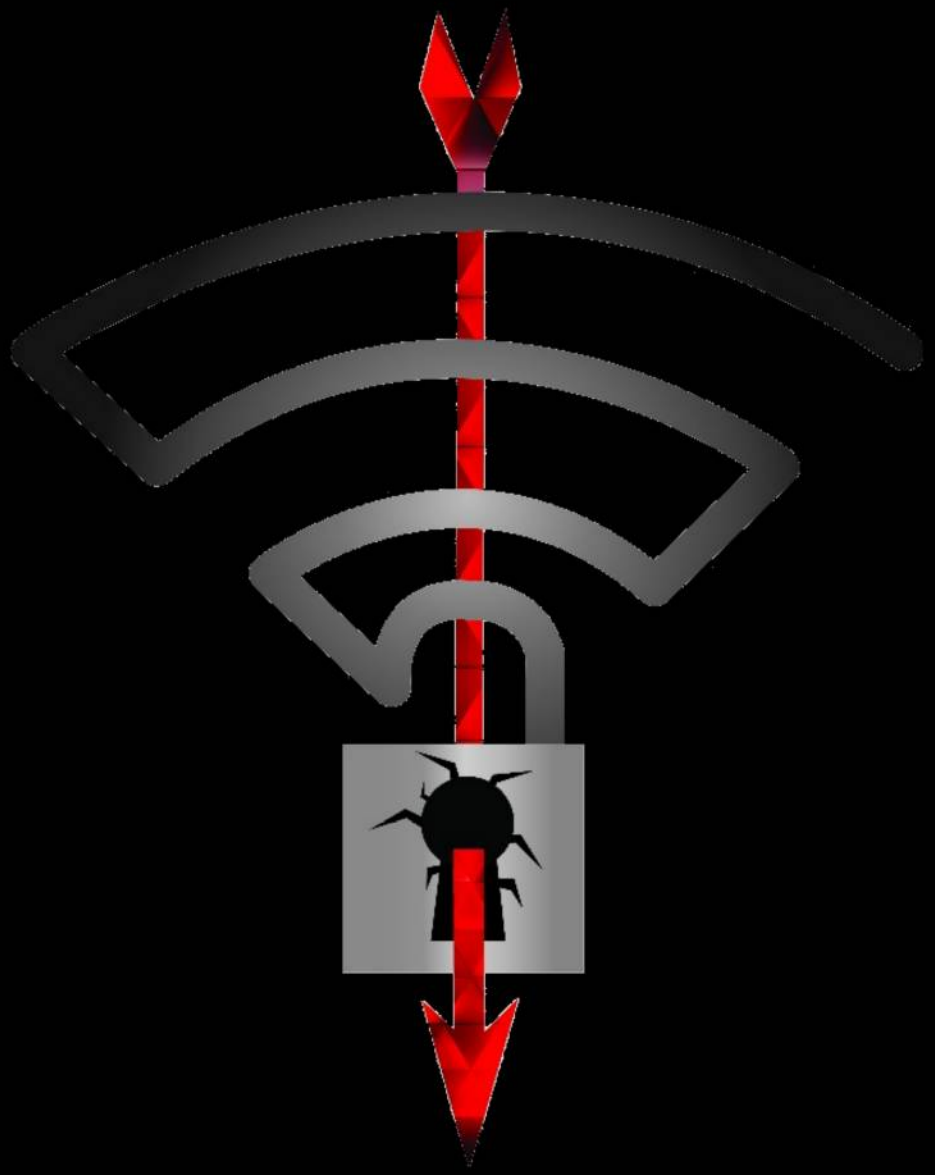


“Relationship Anonymity”
”Traffic Analysis Resistance”

Das Internet



KRACK Attack (2017)



Rogue Access Point

(no logo)

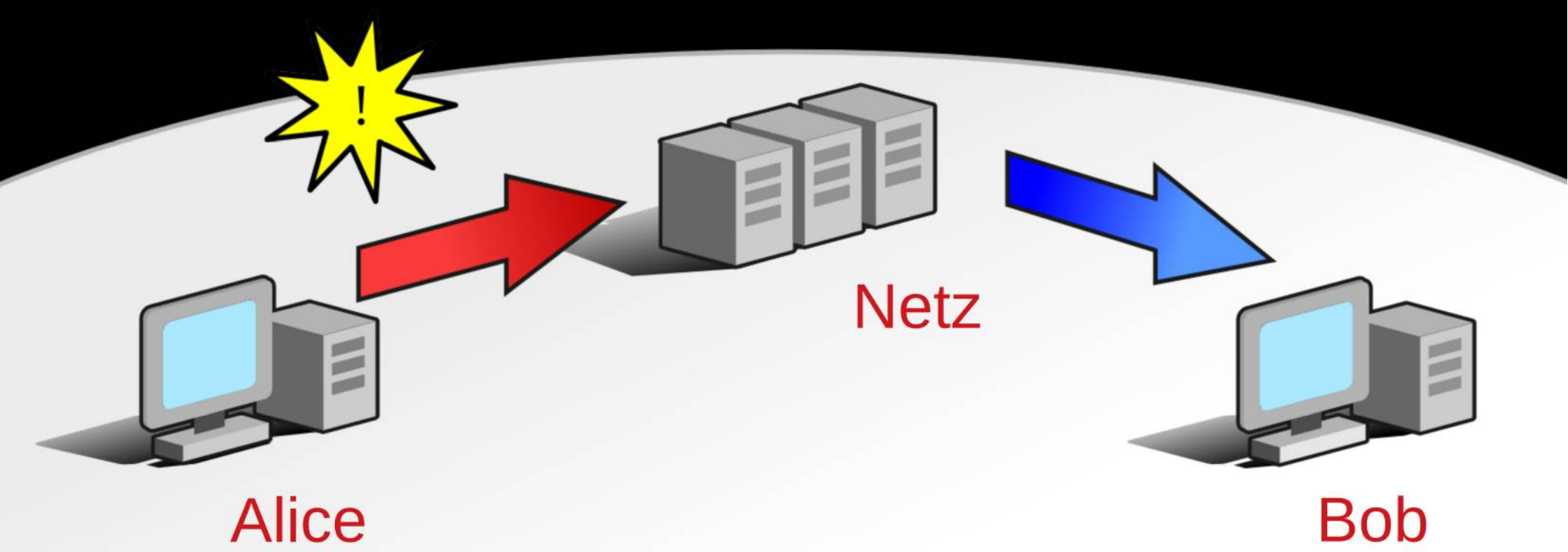
ARP Spoofing

(no logo)

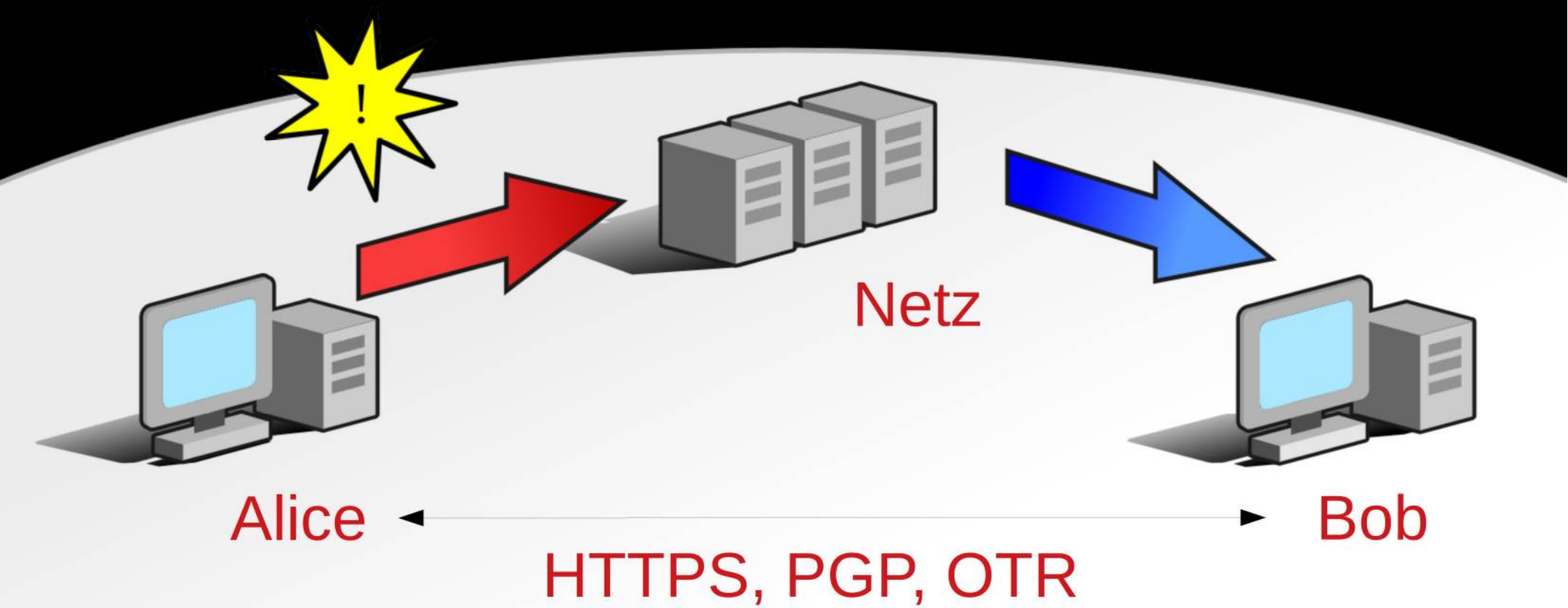
Wifi Brokenness

- Kohlios, Hayajneh: A Comprehensive Attack Flow Model and Security Analysis (2018)

Das Internet



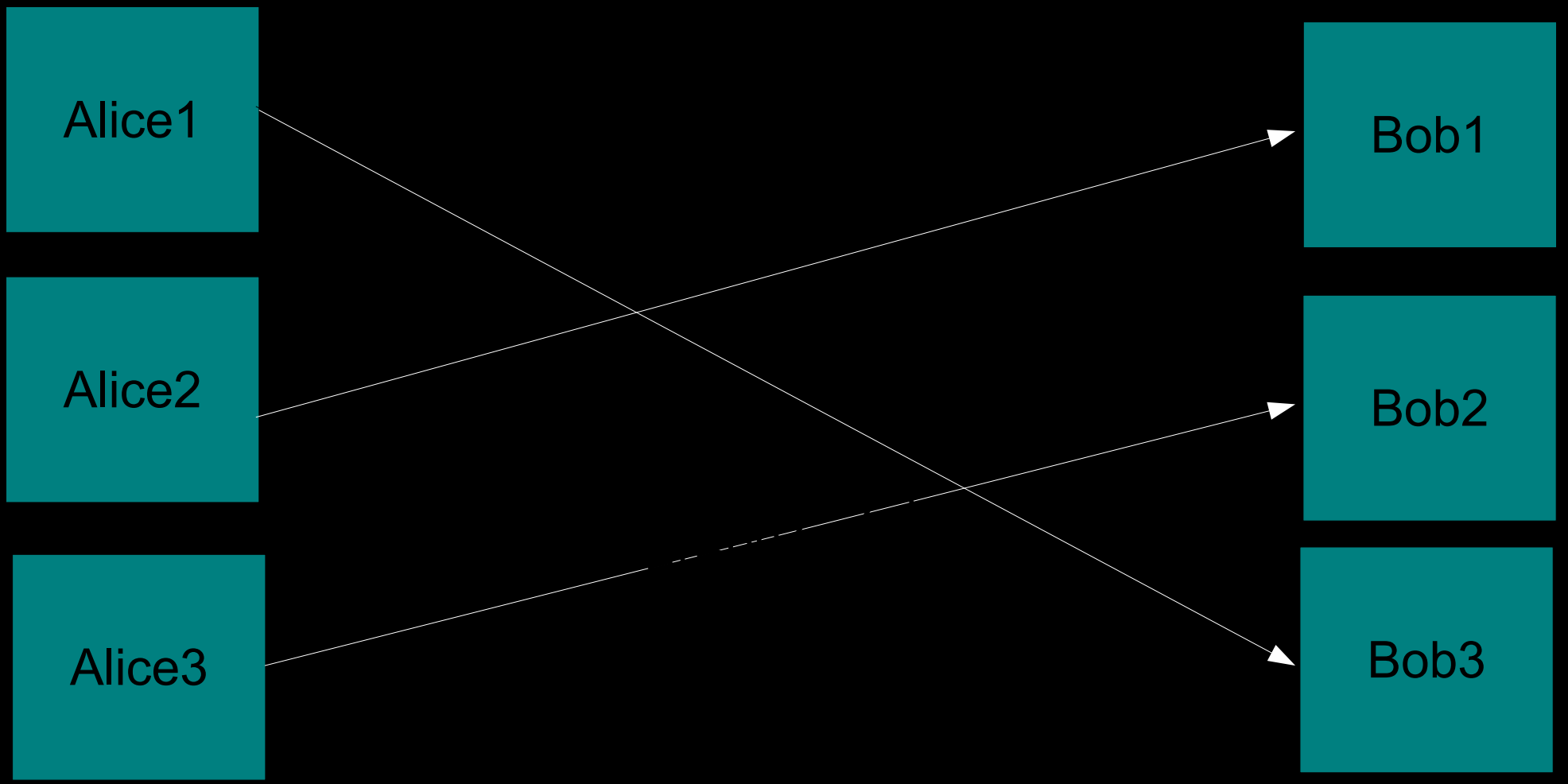
(Ende-zu-Ende) Verschlüsselung



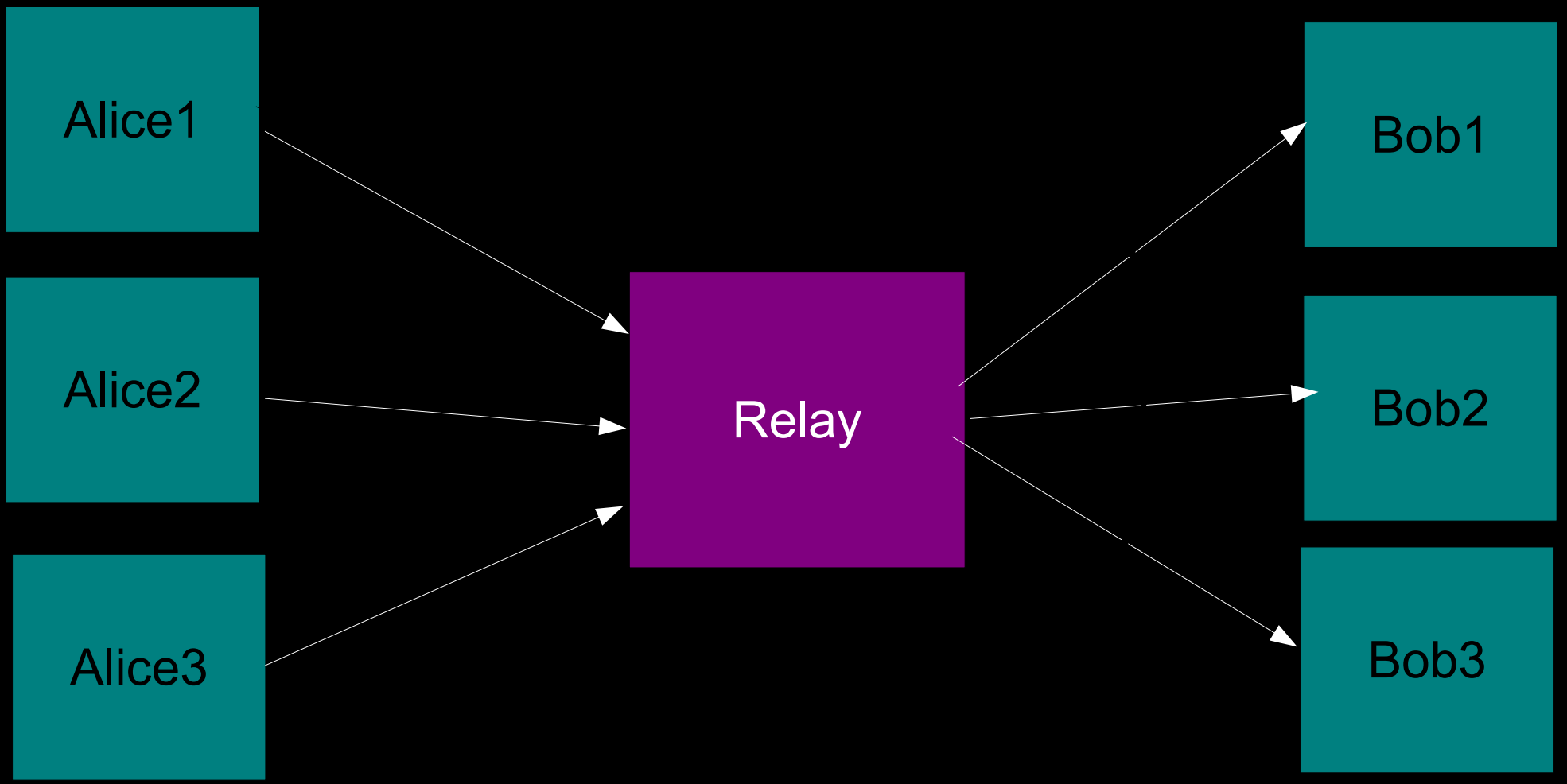
Verschlüsselung schützt nur Inhalte, nicht die Metadaten!

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

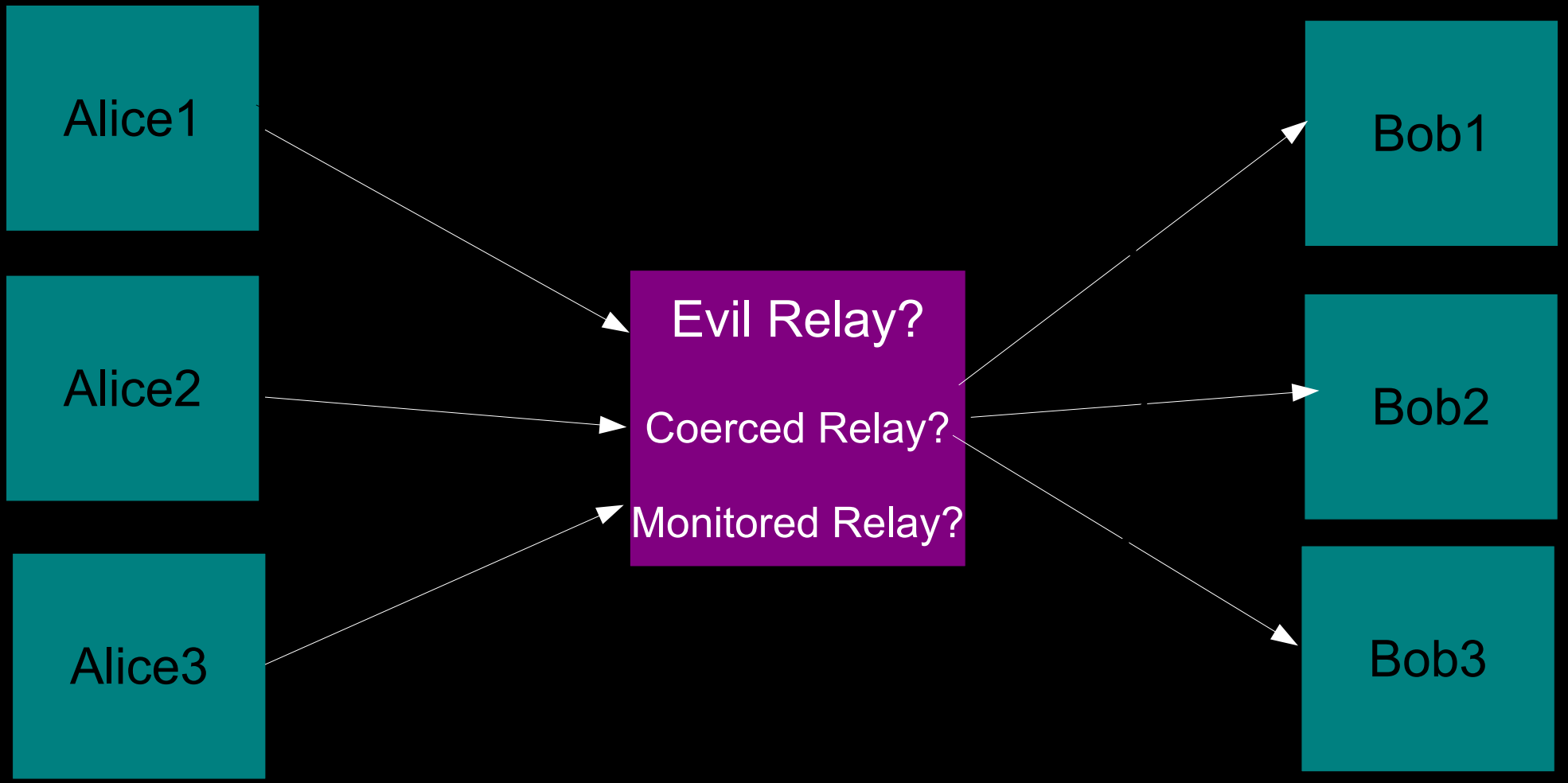
Das Internet
(minimal vereinfachte Darstellung)



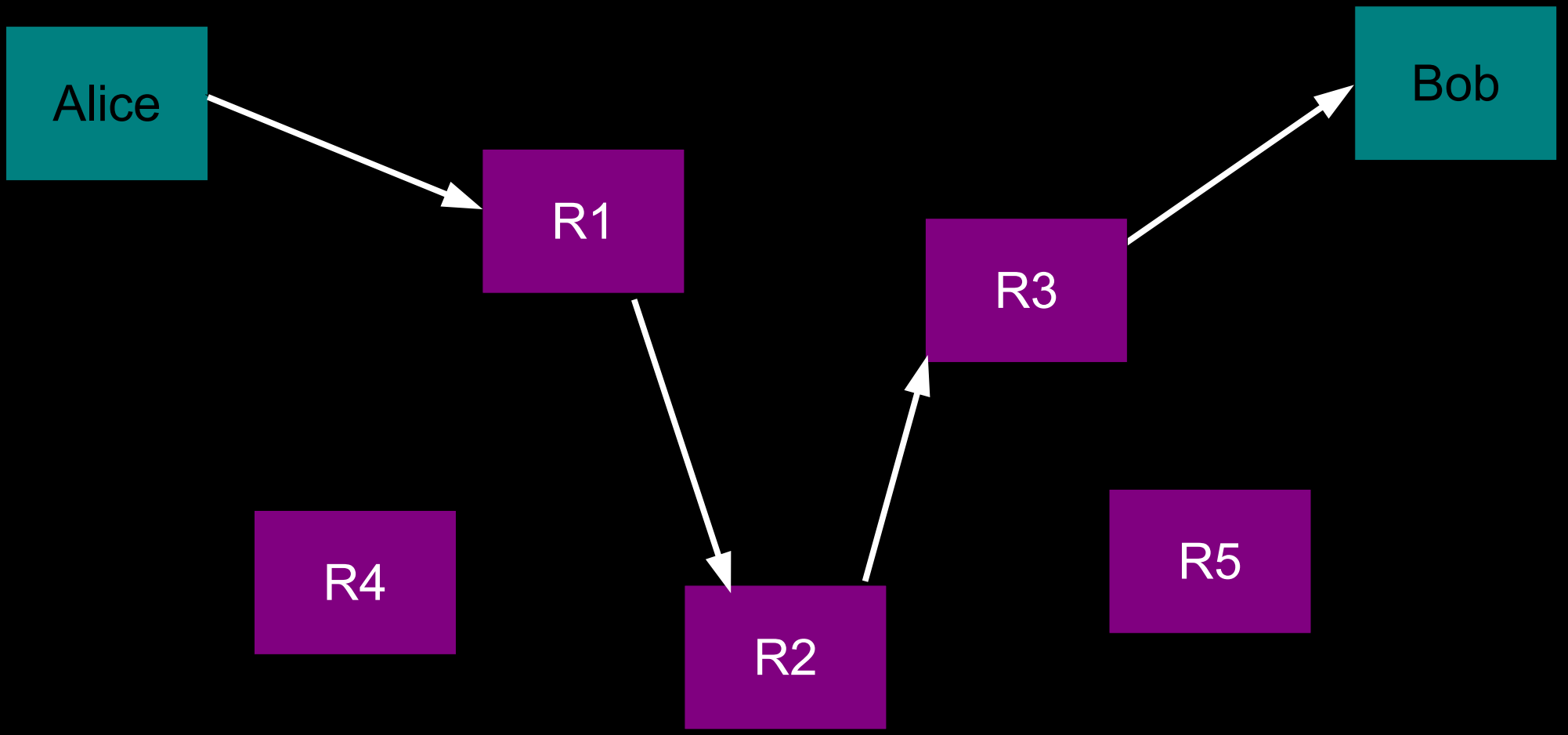
1-hop proxy (VPN, SSH Tunnel etc)



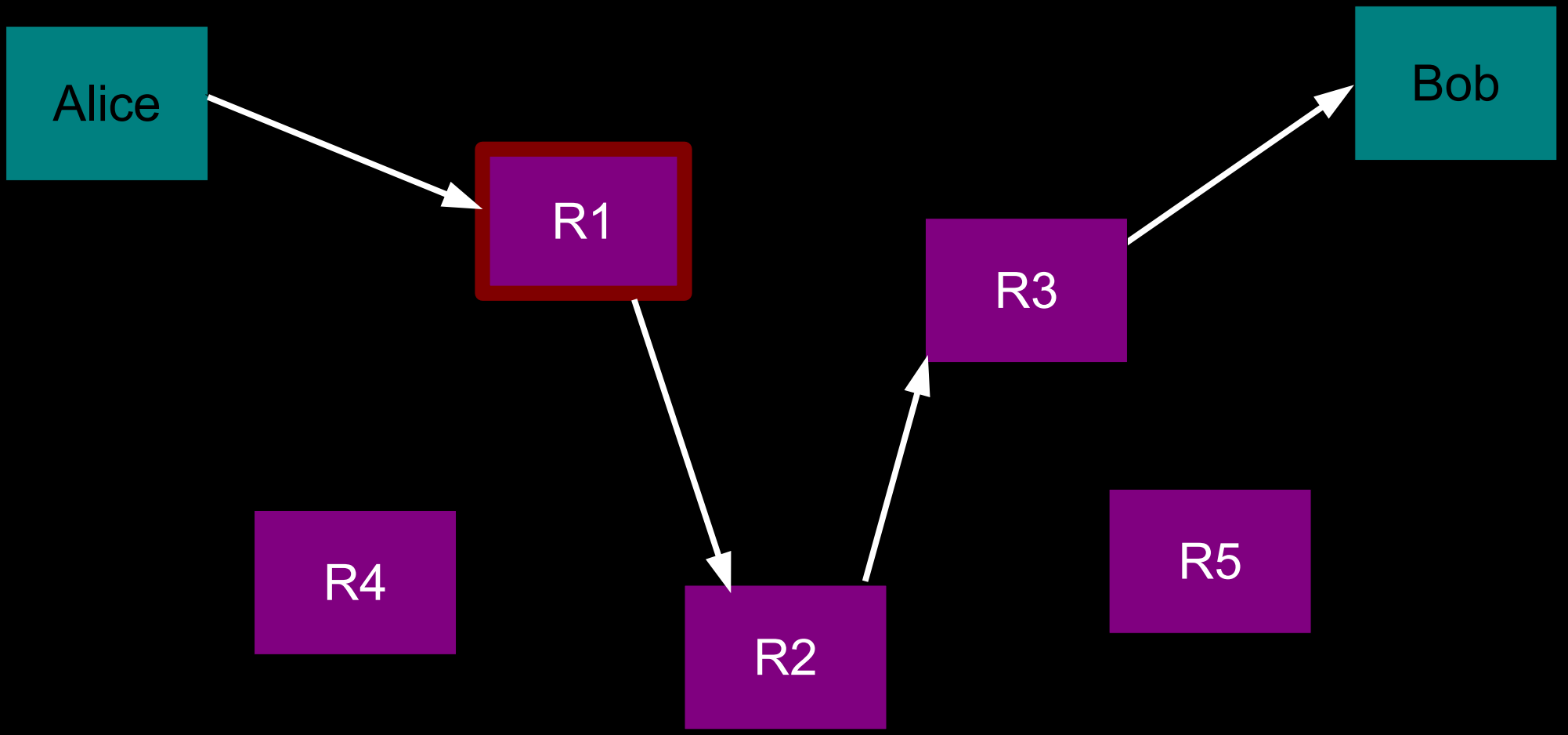
Problem Vertrauenswürdigkeit und einfache Überwachbarkeit



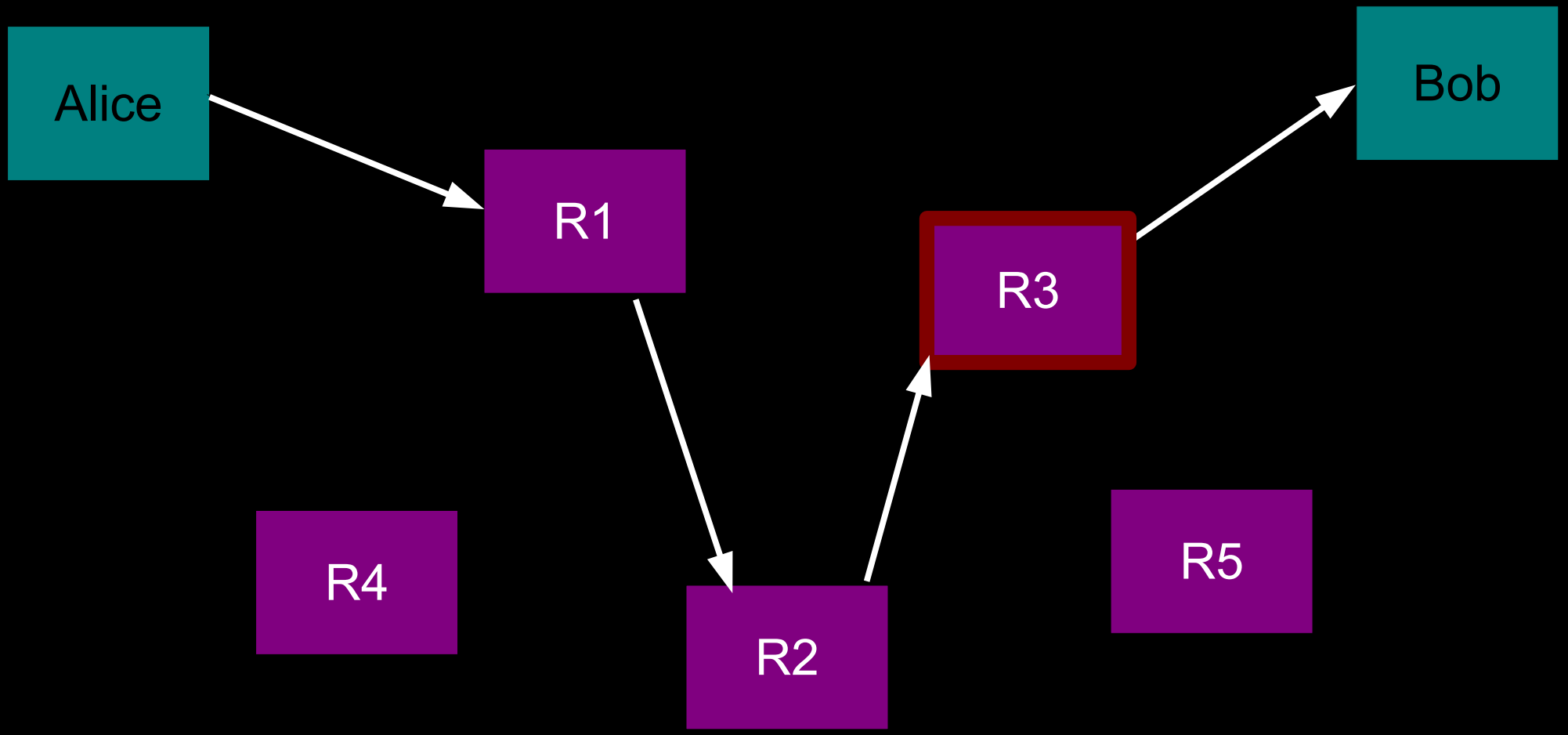
Tor



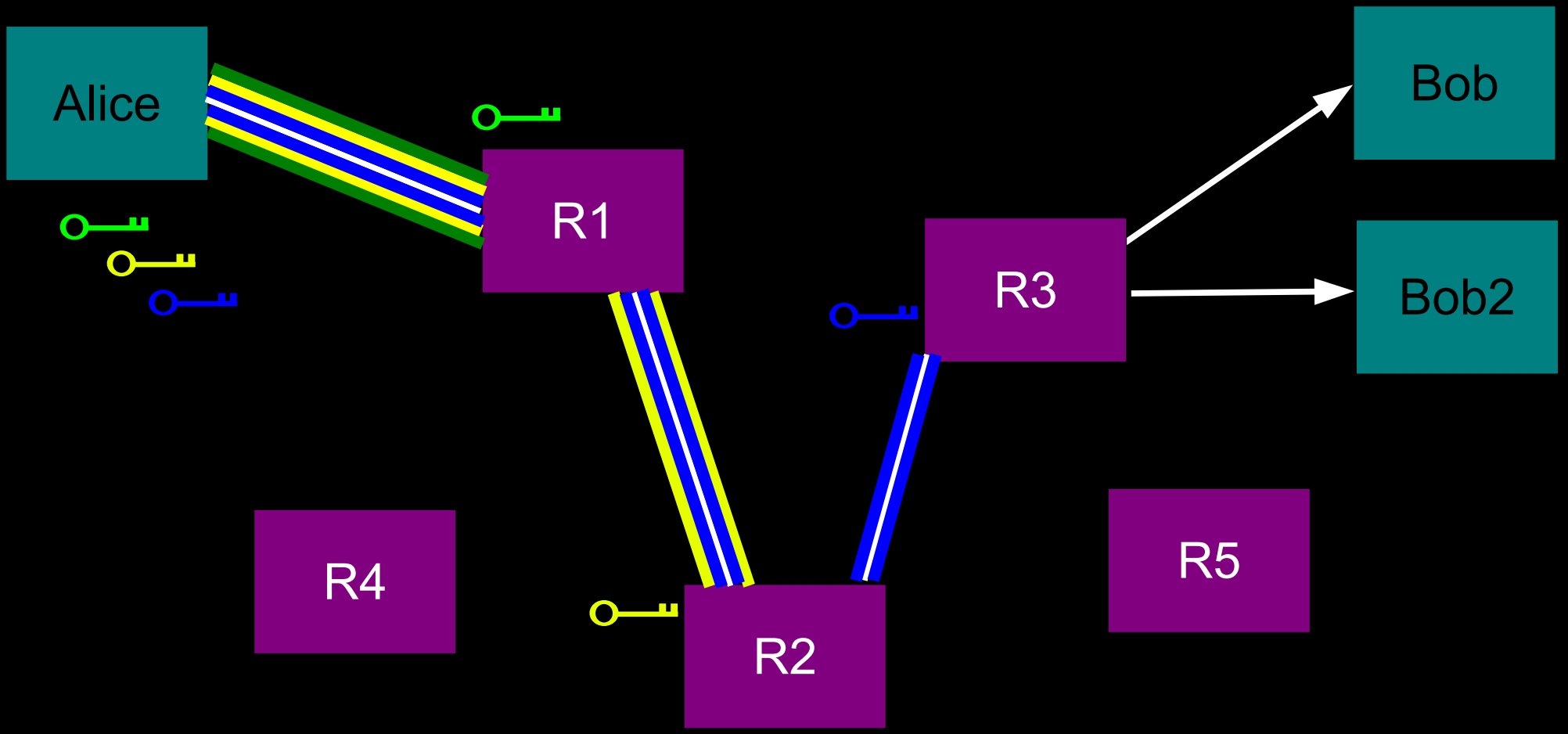
Tor

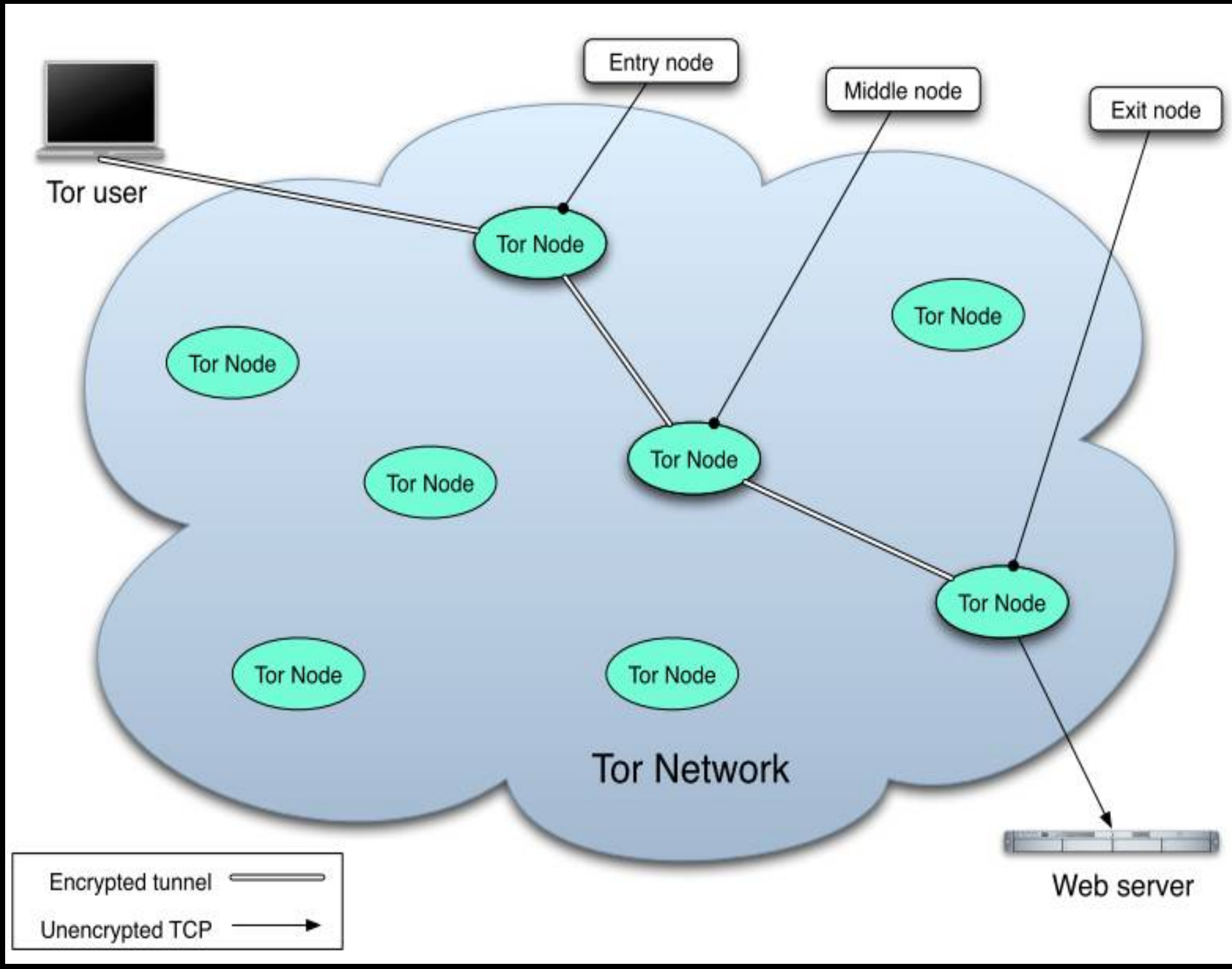


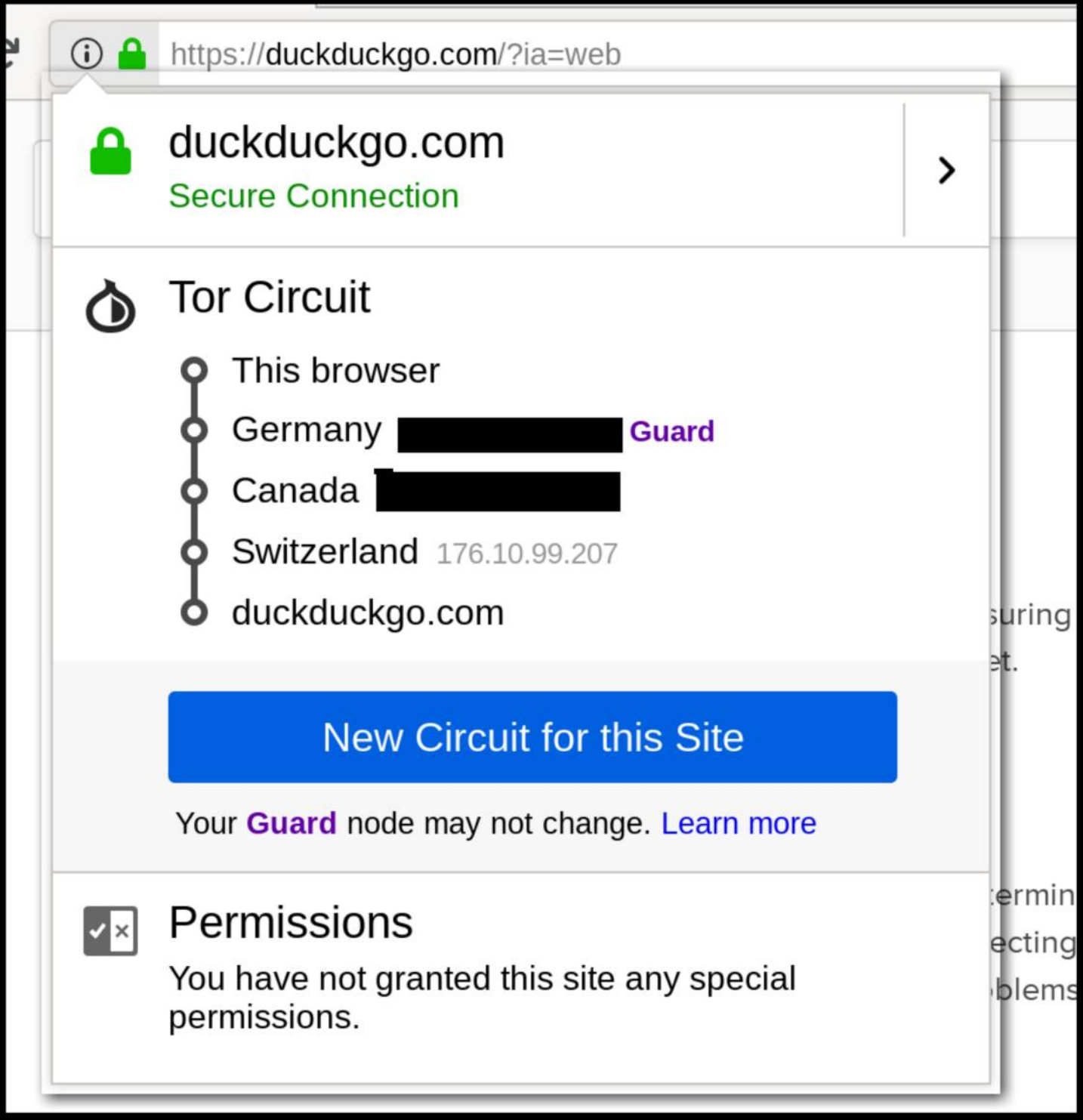
Tor

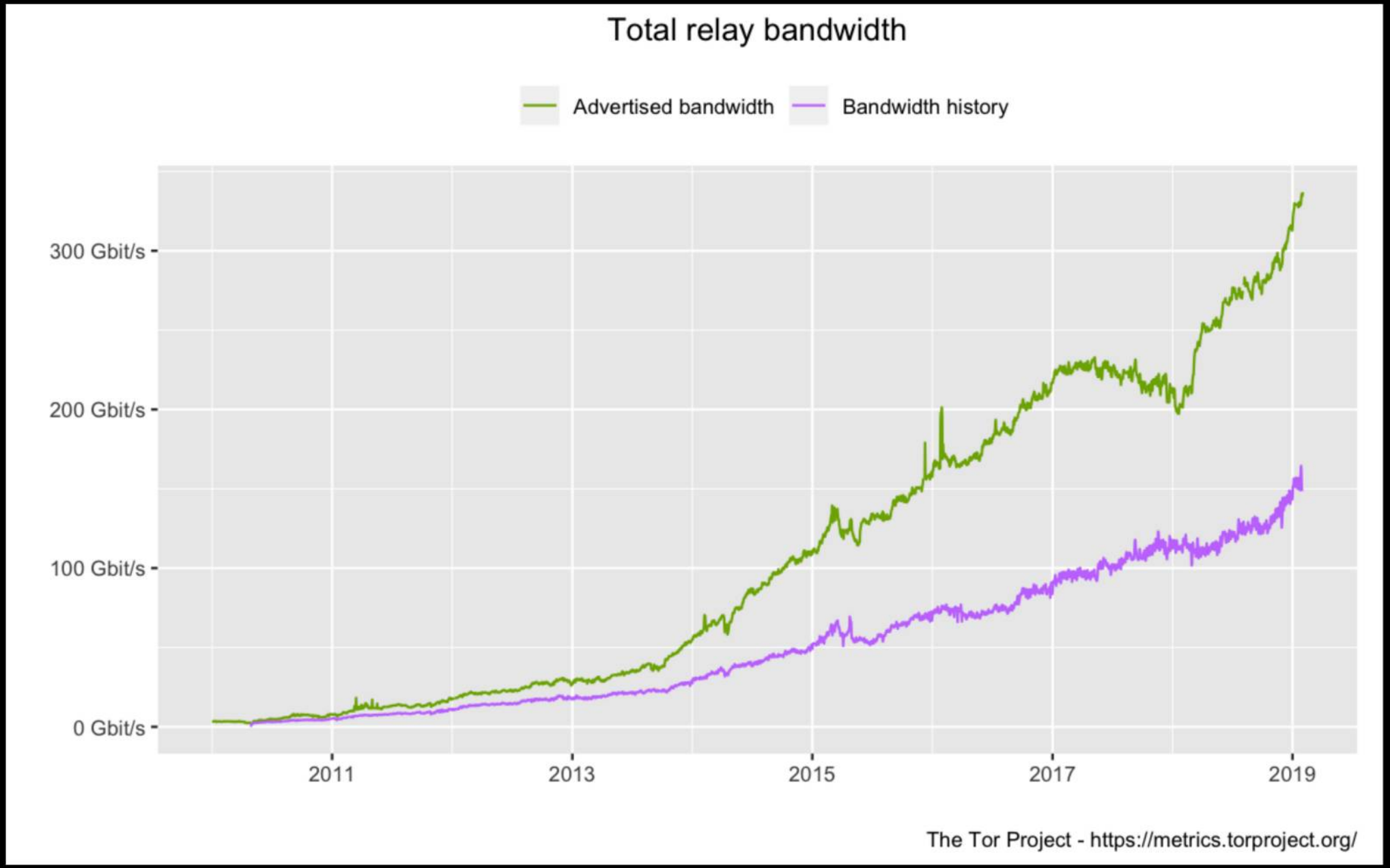


Tor

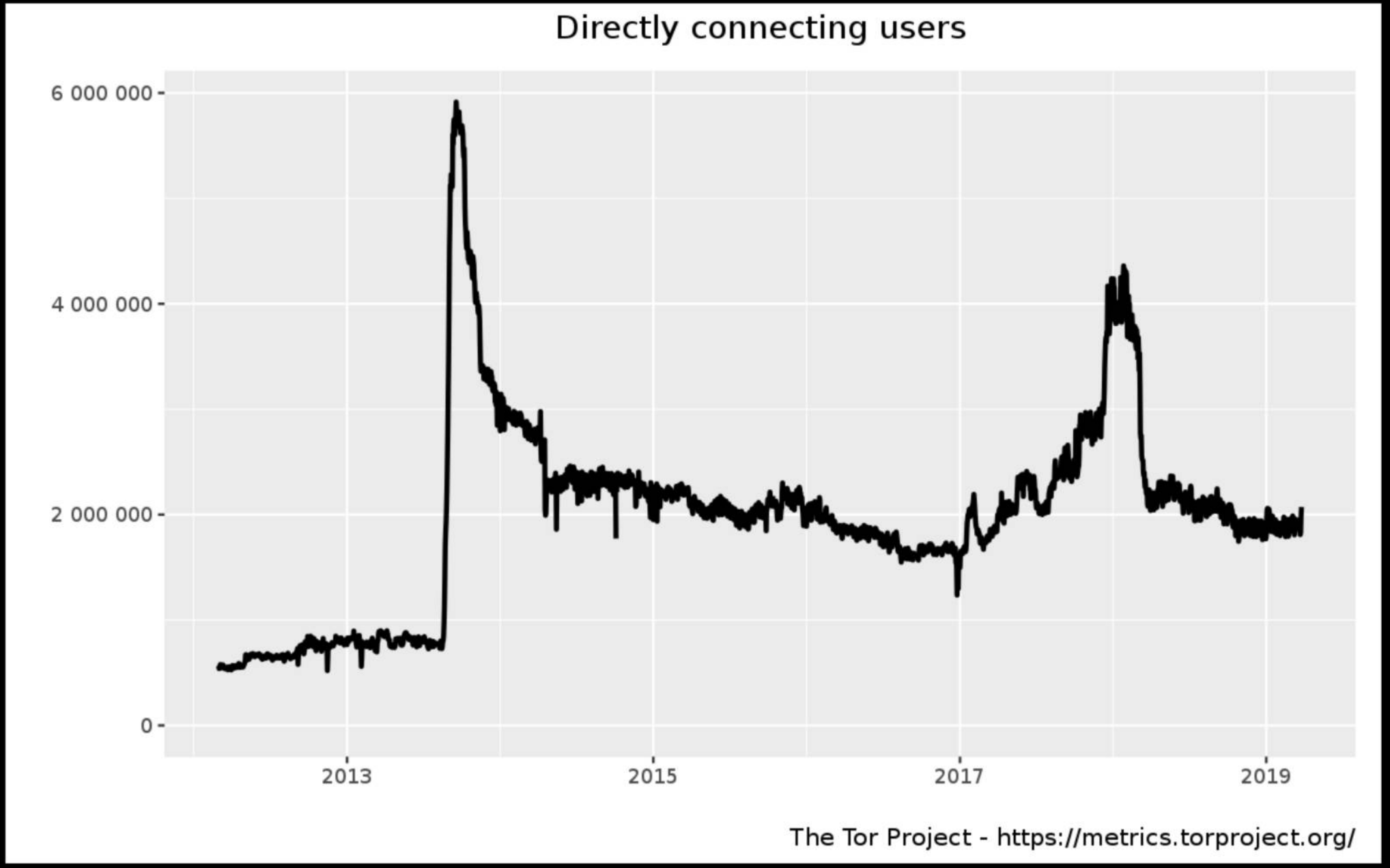



Entry node
Middle node
Exit node
Tor user
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Network
Web server
Encrypted tunnel
Unencrypted TCP


https://duckduckgo.com/?ia=web
duckduckgo.com
Secure Connection
Tor Circuit
This browser
Germany [redacted] Guard
Canada [redacted]
Switzerland 176.10.99.207
duckduckgo.com
New Circuit for this Site
Your Guard node may not change. Learn more
Permissions
You have not granted this site any special permissions.

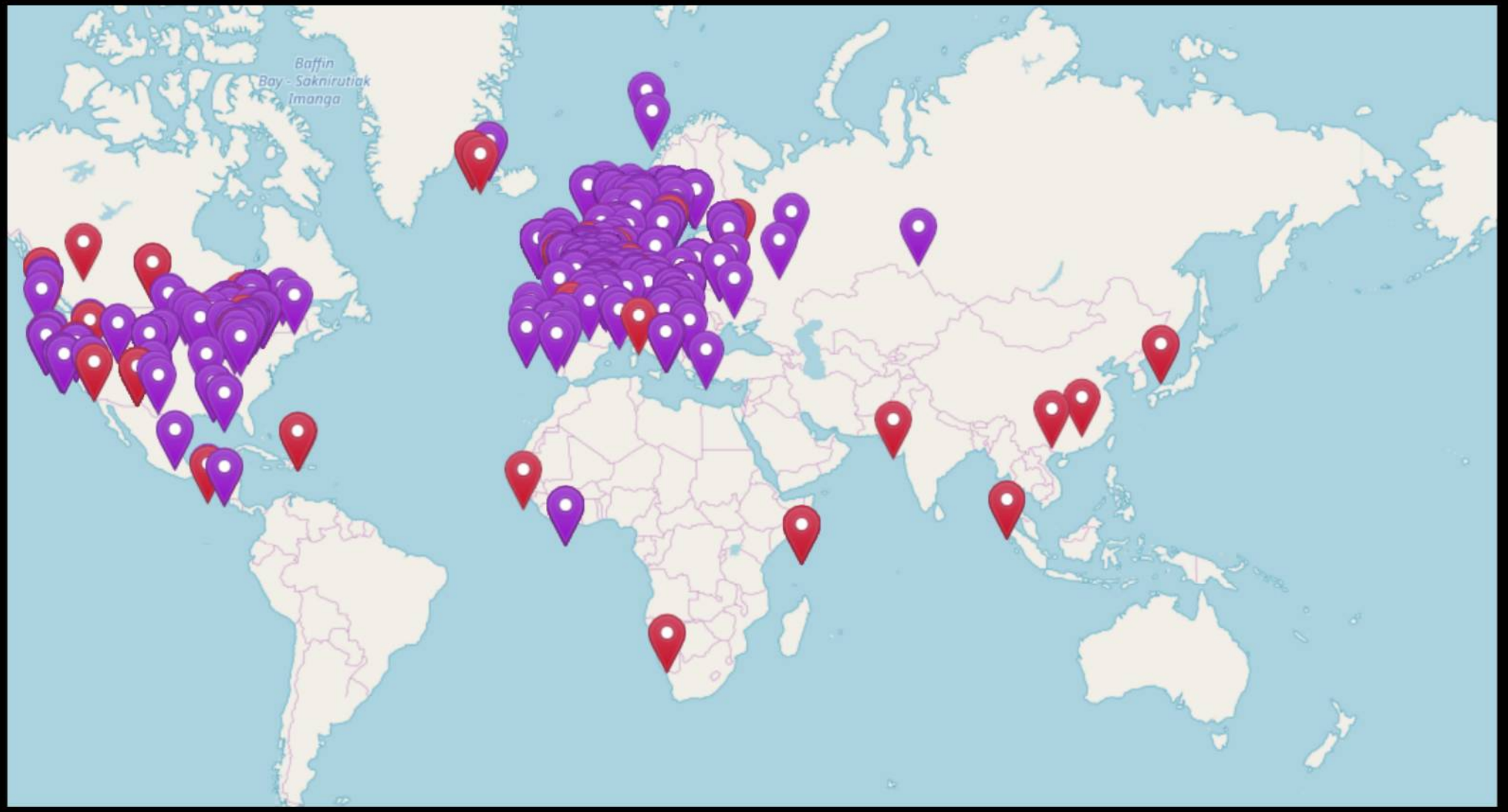

Total relay bandwidth
Advertised bandwidth
Bandwidth history
300 Gbit/s
200 Gbit/s
100 Gbit/s
0 Gbit/s
2011
2013
2015
2017
2019
The Tor Project - https://metrics.torproject.org/

metrics.torproject.org

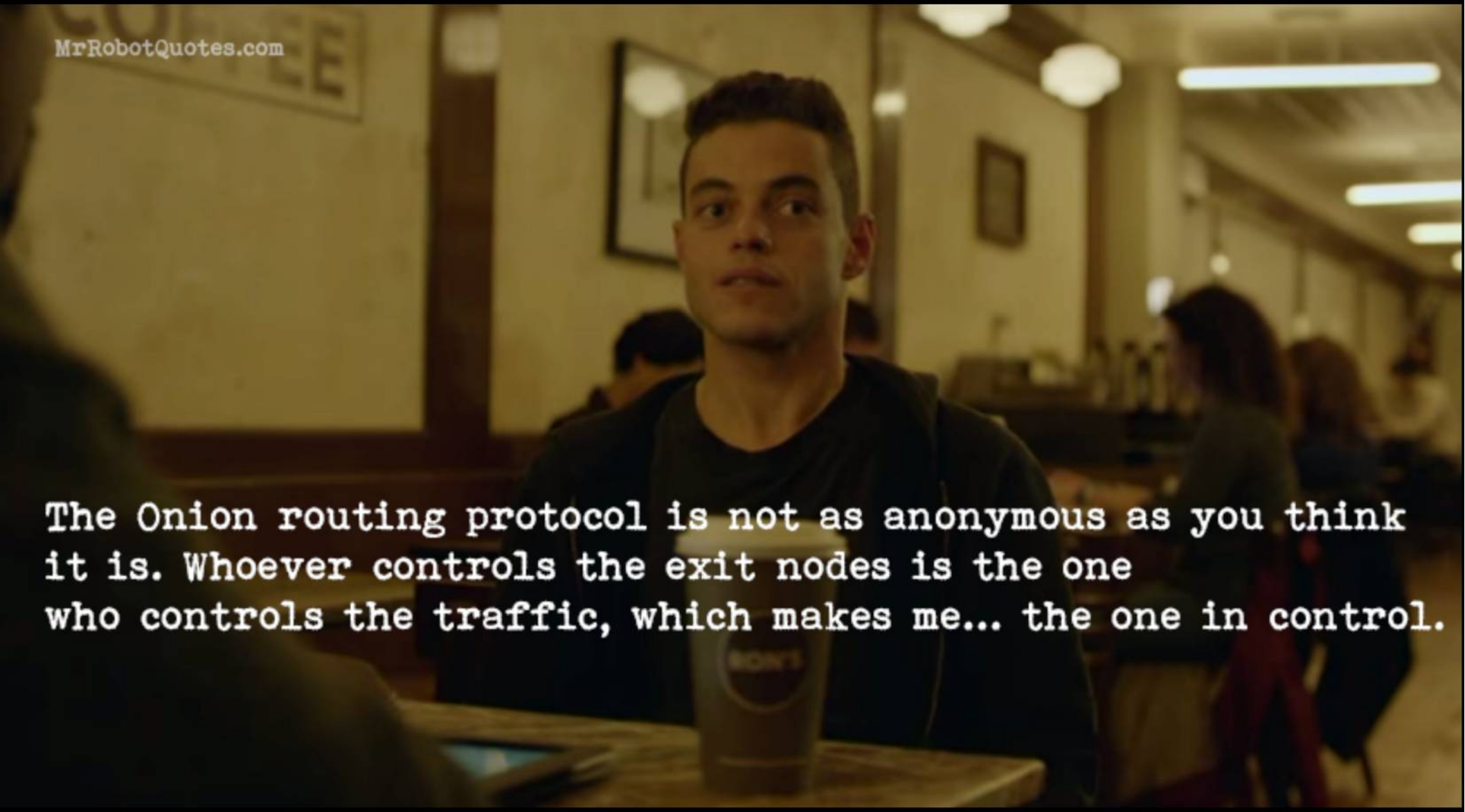


Aktuell: ~7500 Relays, 350 Gbit/s

> 5 Mbit/s



Who runs the relays?



Diversität ...

- Exit Capacity: 11969 MB/s (947 exits)
- Obere 80%: 9575 MB/s (383 exits)

https://github.com/moba/stem-scripts/

Diversität ...

- Exit Capacity: 11969 MB/s (947 exits)
- Obere 80%: 9575 MB/s (383 exits)
  - 156 unterschiedliche ContactInfo strings

https://github.com/moba/stem-scripts/

Diversität ...

- Exit Capacity: 11969 MB/s (947 exits)
- Obere 80%: 9575 MB/s (383 exits)
  - 156 unterschiedliche ContactInfo strings
  - **47** unterschiedliche ContactInfo “fuzzy”

https://github.com/moba/stem-scripts/

Top 10 “Named” Exit Families

ContactInfo	**Exit(%)**	**#Relays**
to-surf-and-protect.net	13.22	44
Zwiebelfreunde	6.3	17
Foundation for Applied Privacy	6.09	9
John L. Ricketts/Quintex	5.02	26
digitale-gesellschaft.ch	2.64	13
ipredator.se	2.29	1
Accessnow.org	1.95	12
Privateinternetaccess.com	1.62	5
tor-network.net	1.61	2
Privacy Republic	1.48	4

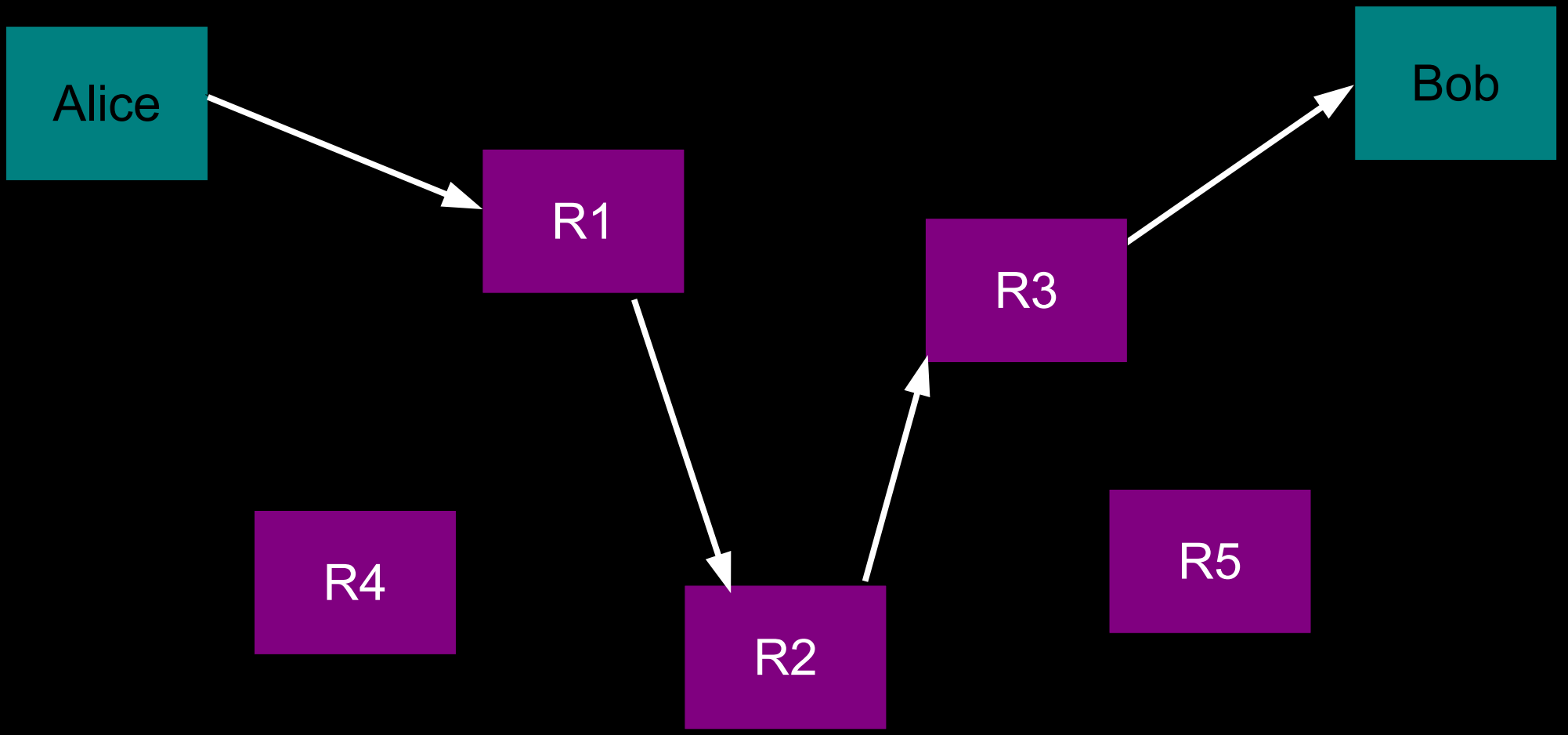
https://nusenu.github.io/OrNetStats/

Top 10 Autonomous Systems

AS Name	Guard(%)	Exit(%)	#Relays
Hetzner Online GmbH	18.13	0.13	420
OVH SAS	16.71	7.84	567
Online S.a.s.	12.91	6.39	319
Joshua Peter McQuistan	0.14	13.22	46
netcup GmbH	2.17	0.66	77
Next Layer GmbH	0.8	6.09	17
iomart Cloud Services Limited.	2.98	0	19
NForce Entertainment B.V.	1.21	3.35	32
myLoc managed IT AG	1.89	0.28	37
SURFnet bv	1.26	2.75	26

https://nusenu.github.io/OrNetStats/

Problem: (sufficiently) global passive adversaries



<Einschub> Der Rechtsstaat

- DE: IT-Sicherheitsgesetz 2.0
  - “Offensive BSI”

- AT: Digitale Vermummung

IT-Sicherheitsgesetz 2.0

- StGB § 126a – Zugänglichmachen von Leistungen zur Begehung von Straftaten

  (1) Wer Dritten eine internetbasierte Leistung zugänglich macht, **deren Zweck oder Tätigkeit darauf ausgerichtet ist, die Begehung von rechtswidrigen Taten zu ermöglichen, zu fördern oder zu erleichtern,** wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

IT-Sicherheitsgesetz 2.0

- StGB § 163g

  Begründen bestimmte Tatsachen den Verdacht, dass jemand Täter oder Teilnehmer einer Straftat im Sinne von § 100g Absatz 1 StPO ist, so dürfen die Staatsanwaltschaft sowie die Behörden und Beamten des Polizeidienstes **auch gegen den Willen des Inhabers auf Nutzerkonten oder Funktionen, die ein Anbieter eines Telekommunikations- oder Telemediendienstes dem Verdächtigen zur Verfügung stellt und mittels derer der Verdächtige im Rahmen der Nutzung des Telekommunikations- oder Telemediendienstes eine dauerhafte virtuelle Identität unterhält, zugreifen. Sie dürfen unter dieser virtuellen Identität mit Dritten in Kontakt treten.** Der Verdächtige ist verpflichtet, die zur Nutzung der virtuellen Identität erforderlichen Zugangsdaten herauszugeben.

IT-Sicherheitsgesetz 2.0

- TKG § 109b – Pflicht der Provider zur Meldung und Löschung

  (1) Stellt der Erbringer öffentlich zugänglicher Telekommunikationsdienste fest, dass sein Dienst zur rechtswidrigen Weitergabe oder Veröffentlichung rechtswidrig erlangter Daten genutzt wird, so hat er unverzüglich das Bundeskriminalamt zu unterrichten.

  (2) Liegen zureichende tatsächliche Anhaltspunkte für eine unrechtmäßige Erlangung oder Verbreitung personenbezogener Daten oder Daten, die Geschäftsgeheimnisse beinhalten, vor, so ist der Zugang zu diesen Daten durch den Diensteerbringer im Sinne des Absatzes 1 zu sperren.

IT-Sicherheitsgesetz 2.0

- TKG §110 (1a) Wer eine Telekommunikationsanlage betreibt, mit der öffentlich zugängliche Telekommunikationsdienste erbracht werden, oder sonst Telekommunikationsdienste erbringt und den Dienst im räumlichen Zuständigkeitsbereich der Bundesnetzagentur anbietet, **hat Daten, zu deren Beauskunftung oder Bereitstellung oder Löschung er nach diesem Abschnitt verpflichtet ist, so zu verarbeiten oder zu speichern, dass er Auskunfts-, Bereitstellungs- oder Löschungsverlangen unmittelbar gegenüber den zuständigen Behörden ausführen kann.**

IT-Sicherheitsgesetz 2.0

- TMG §13: Das Bundesamt für Sicherheit in der Informationstechnik kann zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes oder eines Betreibers einer Kritischen Infrastruktur oder für eine Infrastruktur im besonderen öffentlichen Interesse gegenüber Diensteanbietern in begründeten Ausnahmefällen **die Umsetzung erforderlicher technischer und organisatorischer Vorkehrungen zur Sicherstellung der Schutzgüter** nach Absatz 7 Satz 1 **anordnen**, wenn hierdurch eine konkrete Gefahr für Datenverarbeitungssysteme einer Vielzahl von Nutzern durch unzureichend gesicherte Telemedienangebote beseitigt werden kann.

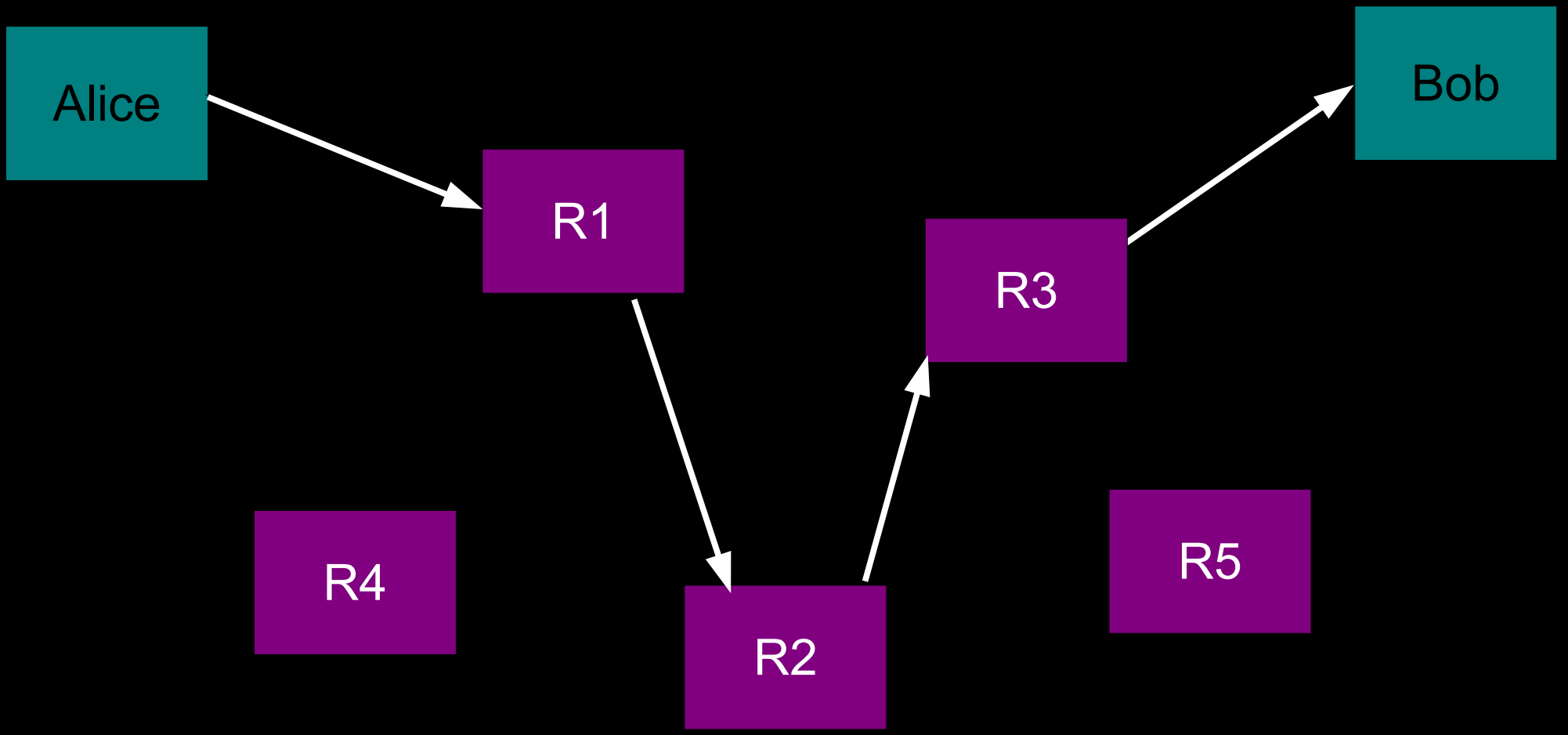
(AT, 2020) “Vermummungsverbot”

- Identifizierungspflicht
  - Ab 100k registrierten Nutzern

    oder
  - Umsatz > 500k€

    oder
  - Presseförderung > 50k€
- Nicht im Widerspruch mit “Anonymisierung”?

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.)

“There is clear evidence that timing information is both recognized as being key to correlating events and streams; and it is being recorded and stored at an increasing granularity. There is no smoking gun as of 2011 to say they casually de-anonymize Tor circuits, but the writing is on the wall for the onion routing system. **GCHQ at 2011 had all ingredients needed to trace Tor circuits. It would take extra-ordinary incompetence to not have refined their traffic analysis techniques in the past 5 years.** The Tor project should do well to not underestimate GCHQ’s capabilities to this point.

[…] One should wonder why we have been waiting for 3 years until such clear documents are finally being published from the Snowden revelations. If those had been the first published, instead of the obscure, misleading and very non-informative slides, it would have saved a lot of time — and may even have engaged the public a bit more than bad powerpoint.”

George Danezis, “A technical reading of the HIMR Data Mining Research Problem Book”, February 3rd 2016 – https://conspicuouschatter.wordpress.com/2016/02/03/a-technical-reading-of-the-himr-data-mining-research-problem-book/

DeepCorr (August 2016)

"We show that with moderate learning, DeepCorr can correlate Tor connections (and therefore break its anonymity) with accuracies significantly higher than existing algorithms, and using substantially shorter lengths of flow observations. For instance, **by collecting only about 900 packets of each target Tor flow (roughly 900KB of Tor data), DeepCorr provides a flow correlation accuracy of 96%** compared to 4% by the state-of-the-art system of RAPTOR using the same exact setting."

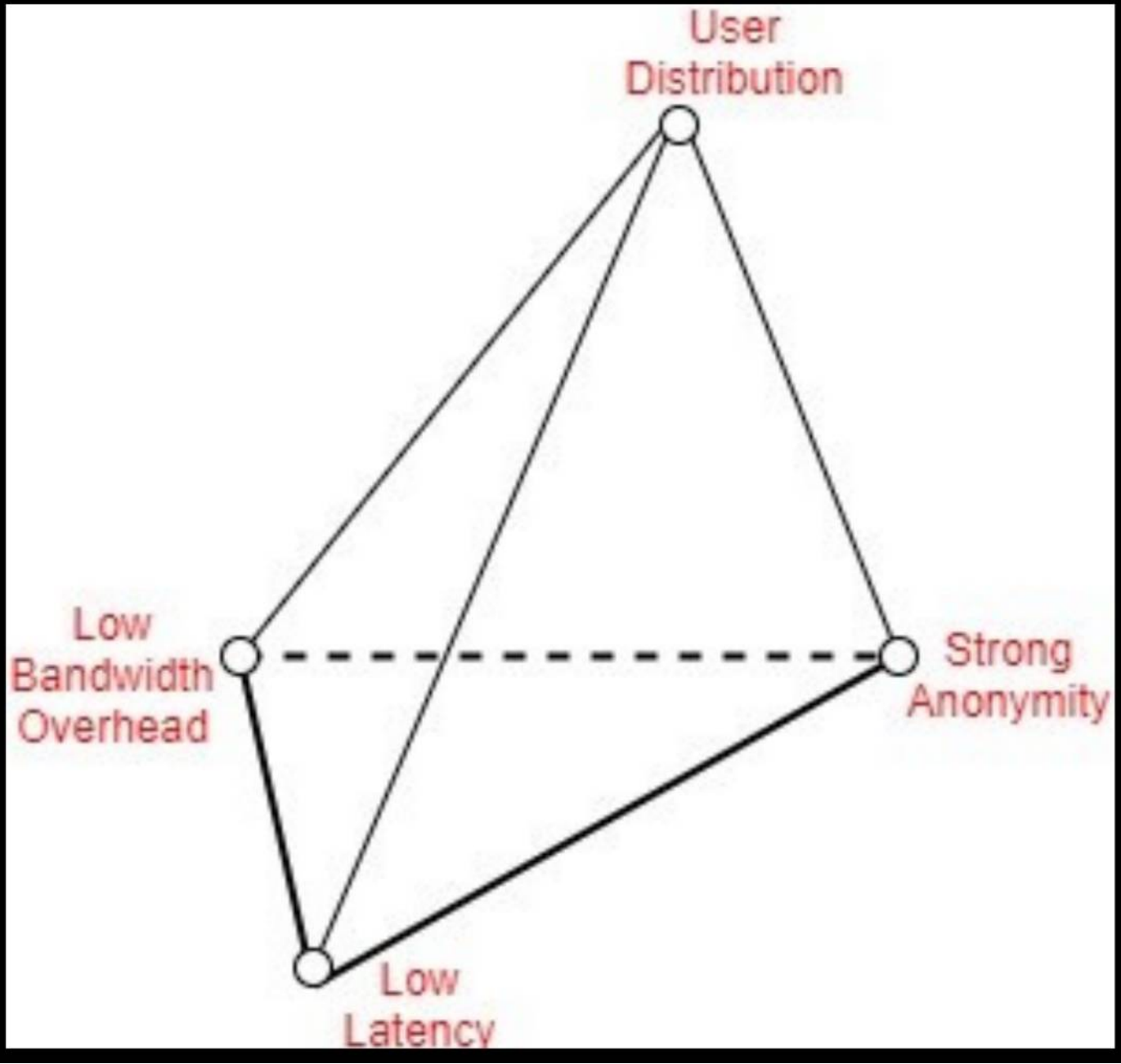
https://arxiv.org/abs/1808.07285

OK NOW WHAT?

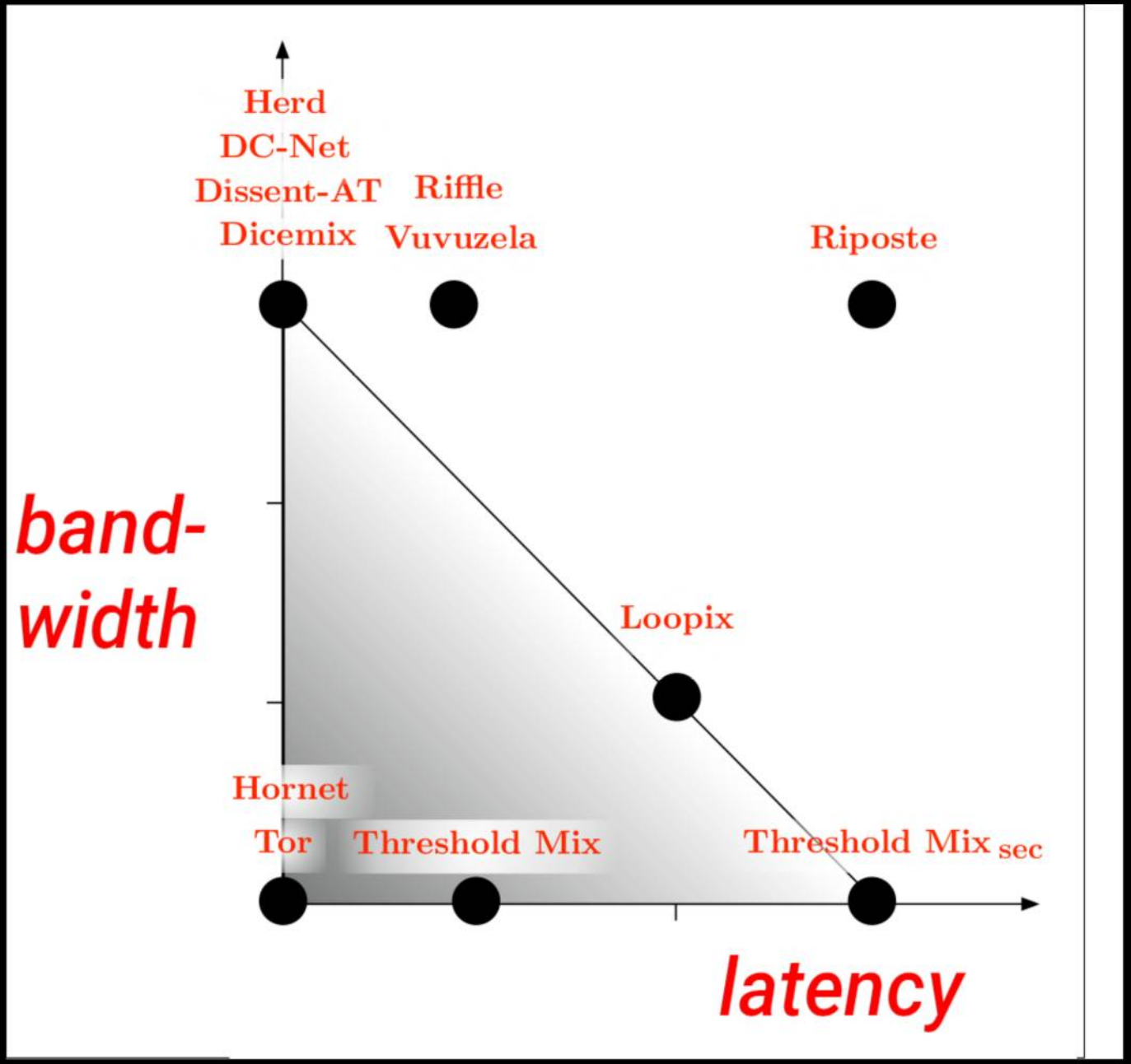
David Stainton: Learn Mix Networks for Great Good

https://katzenpost.mixnetworks.org/docs/mixnet_academy/syllabus.html

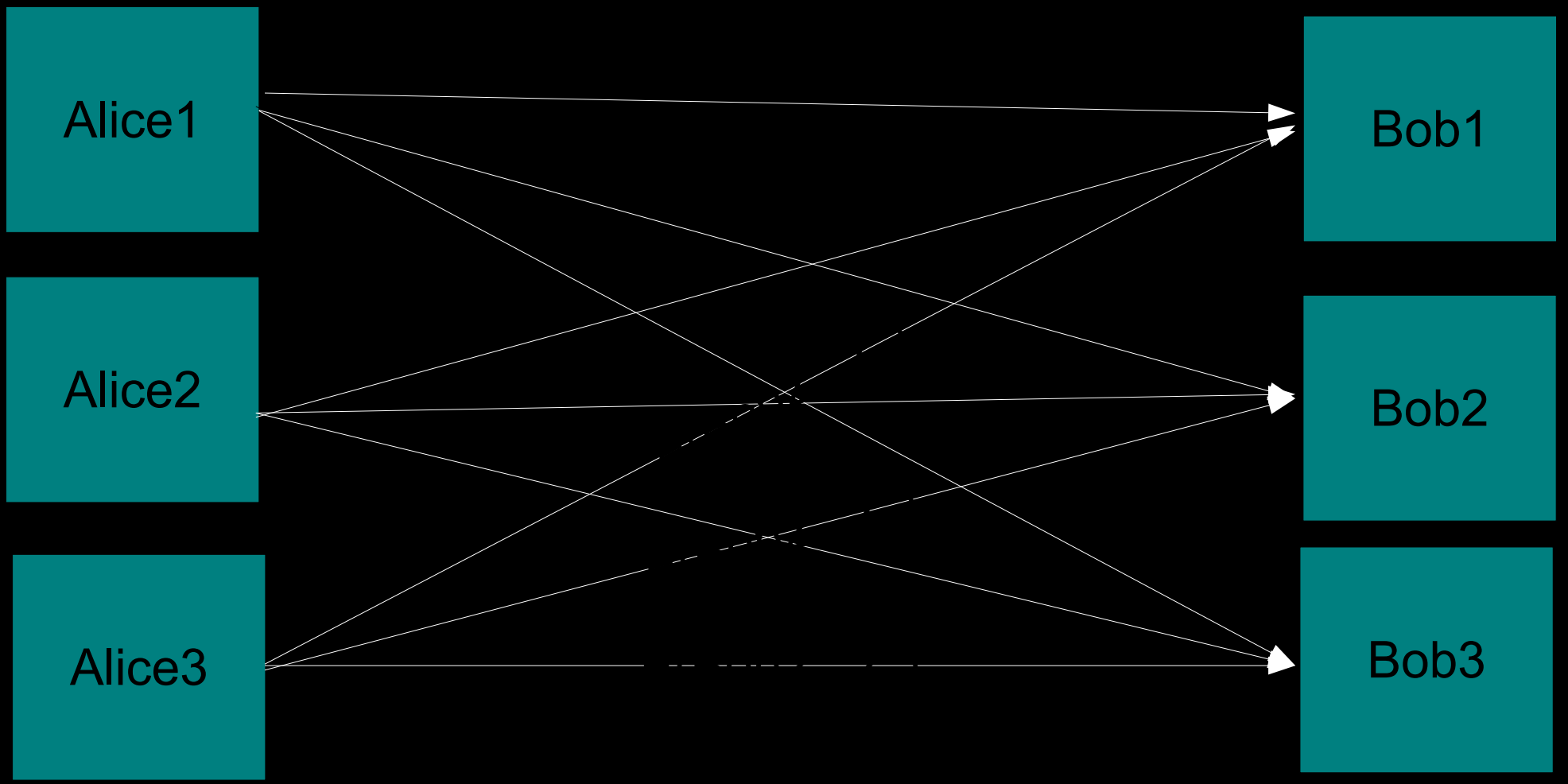
“Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency—Choose Two”



“Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency—Choose Two”



Alternative: Broadcast-Architektur



Beispiel Bitmessage

Dining Cryptographers (DC-Netze)

- “rundenbasiert”
- Dissent (2012)

Dining Cryptographers

- Dissent (2012)

  when multiple users wish to communicate simultaneously, every user must transfer a message of size proportional to the number of clients who wish to communicate.

Dining Cryptographers

- Dissent (2012)

  when multiple users wish to communicate simultaneously, every user must transfer a message of size proportional to the number of clients who wish to communicate.
- PriFi

Riffle (2006)

- Verifiable Shuffles

Riffle (2006)

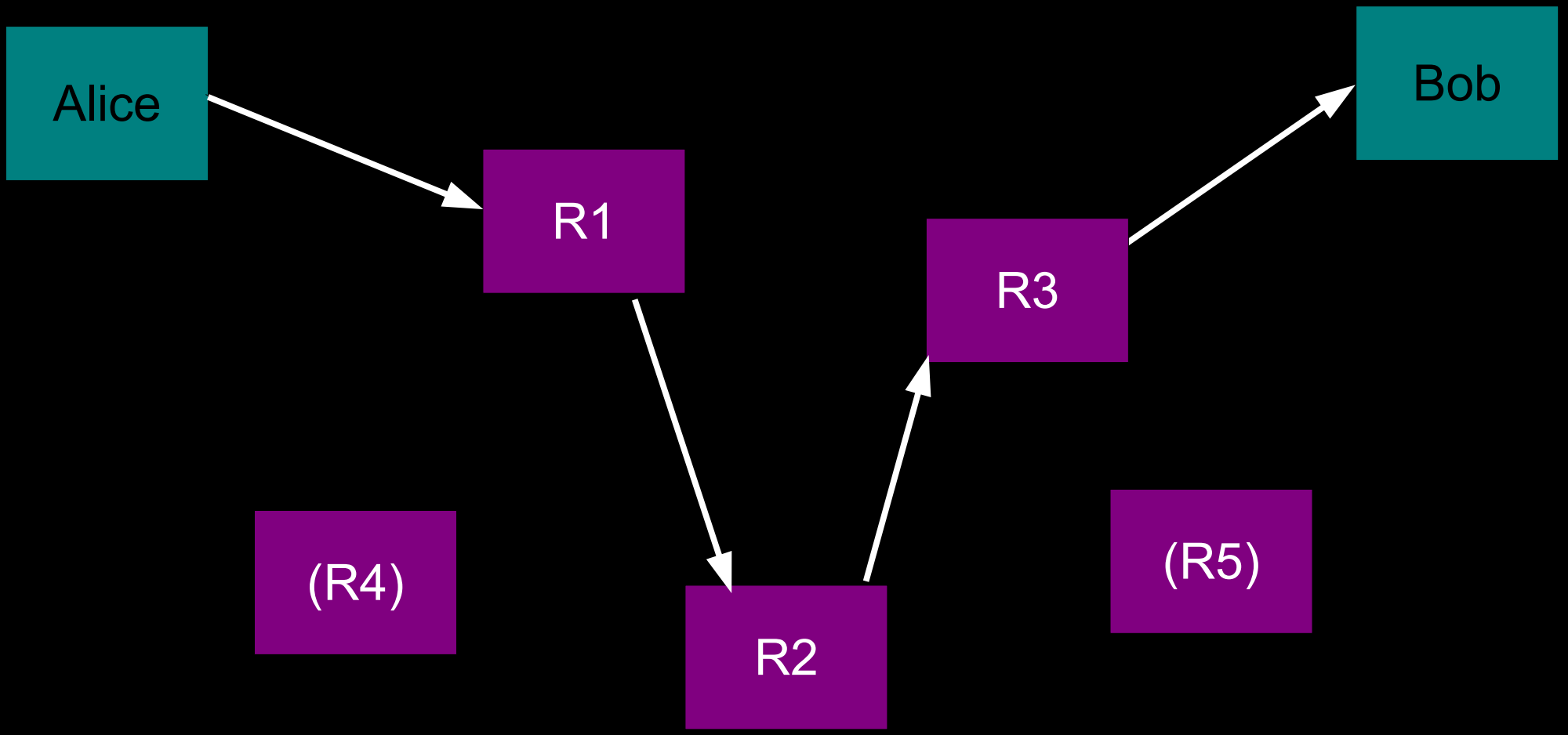
- Verifiable Shuffles
- (Unlösbares?) Problem: “Churn” / Veränderungen im Netz
  - wechselnde/neue Nutzer
  - wechselnde/neue Relays

HORNET / TARANET

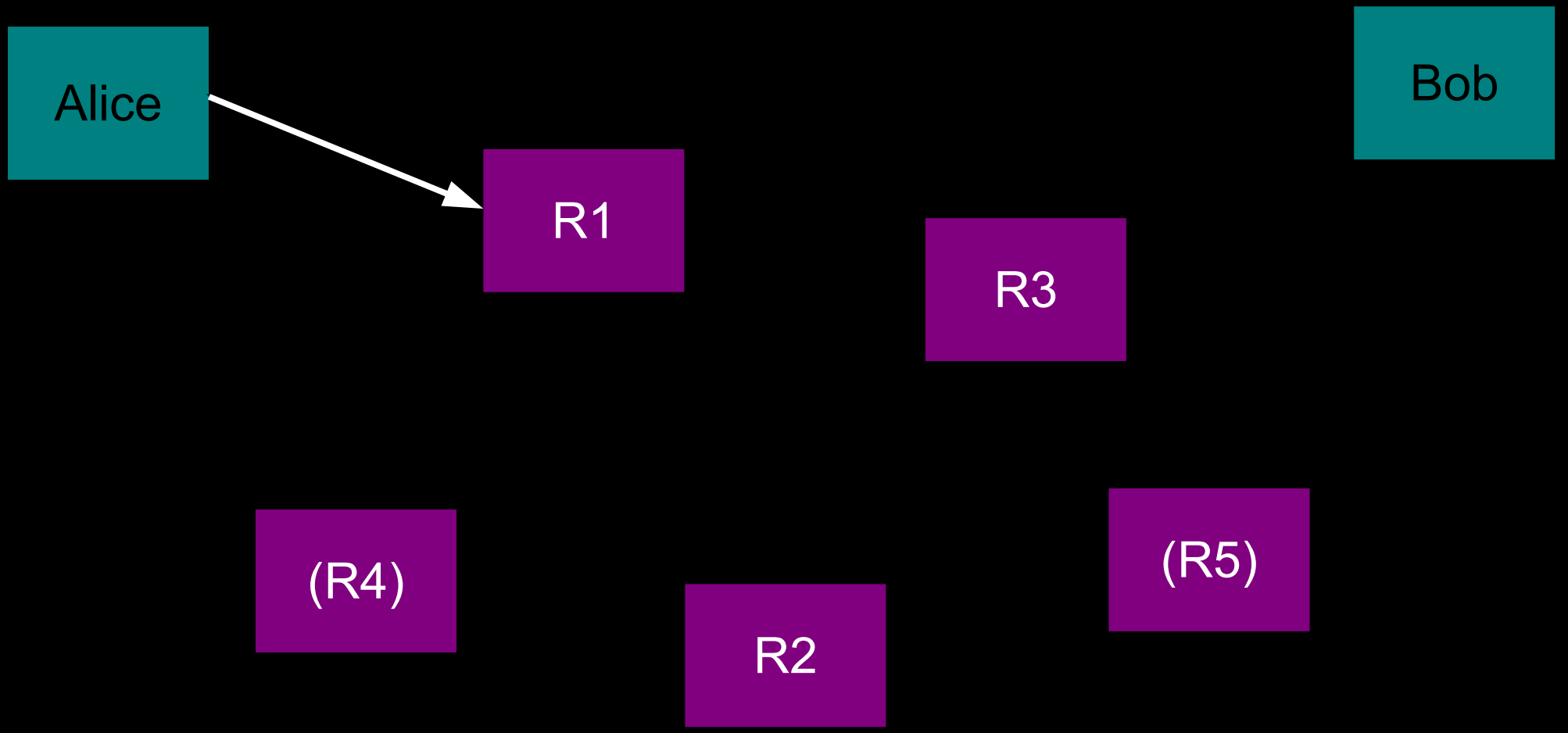
- (LAP, Dovetail, Hornet, Taranet)
- Network layer, kein Overlay

  → realistisch?

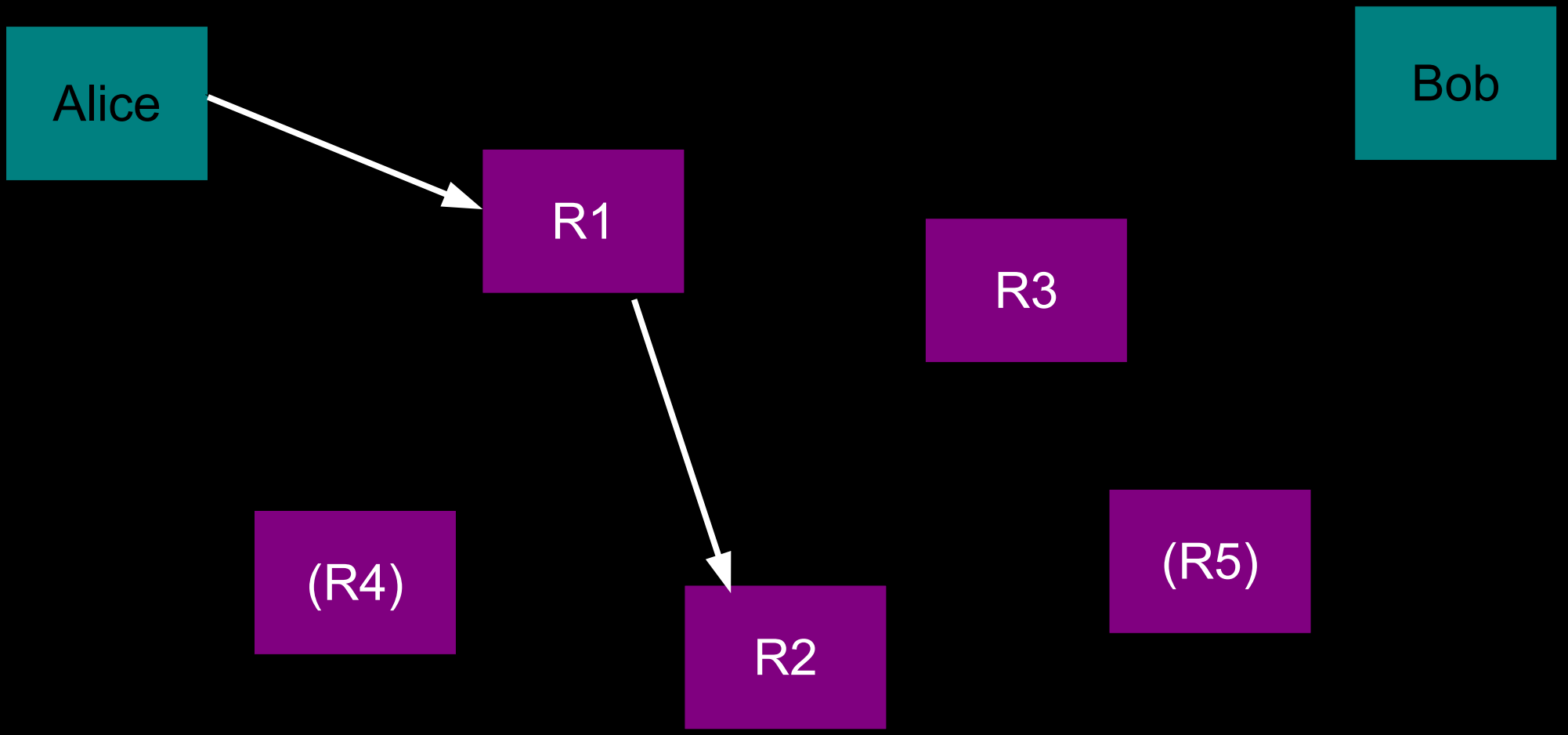
Alternative: Mixnets



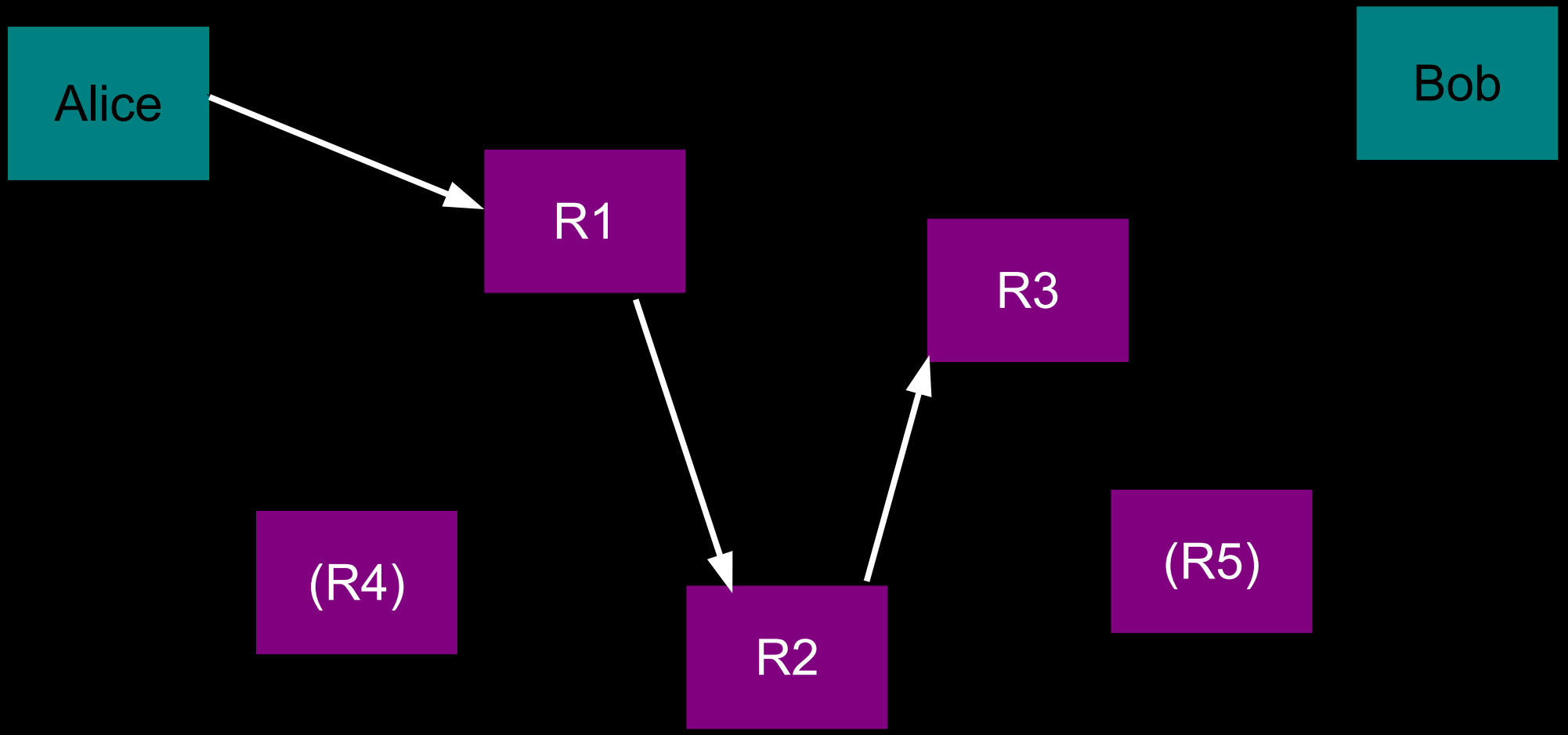
Tor: Verbindungsaufbau



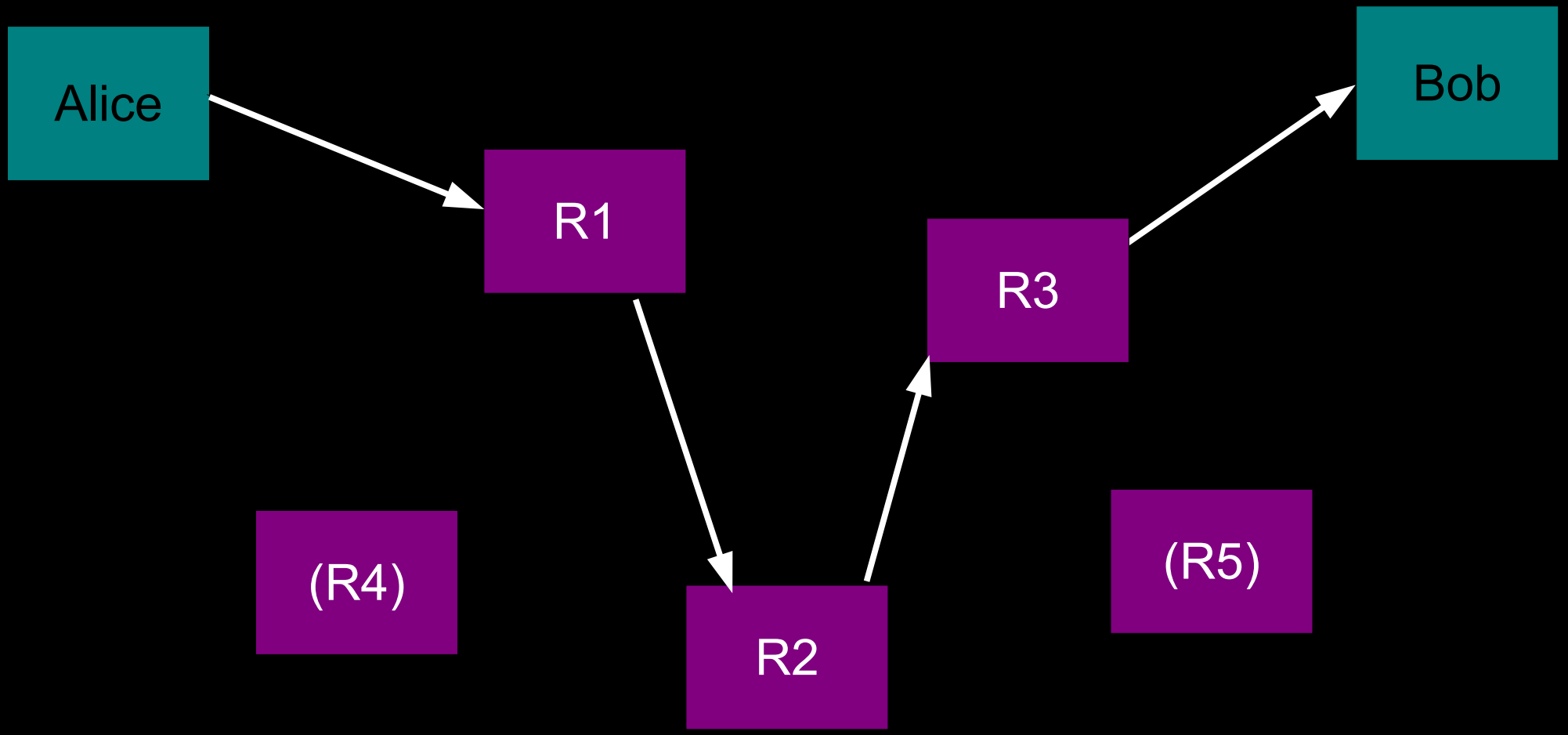
Tor: Verbindungsaufbau



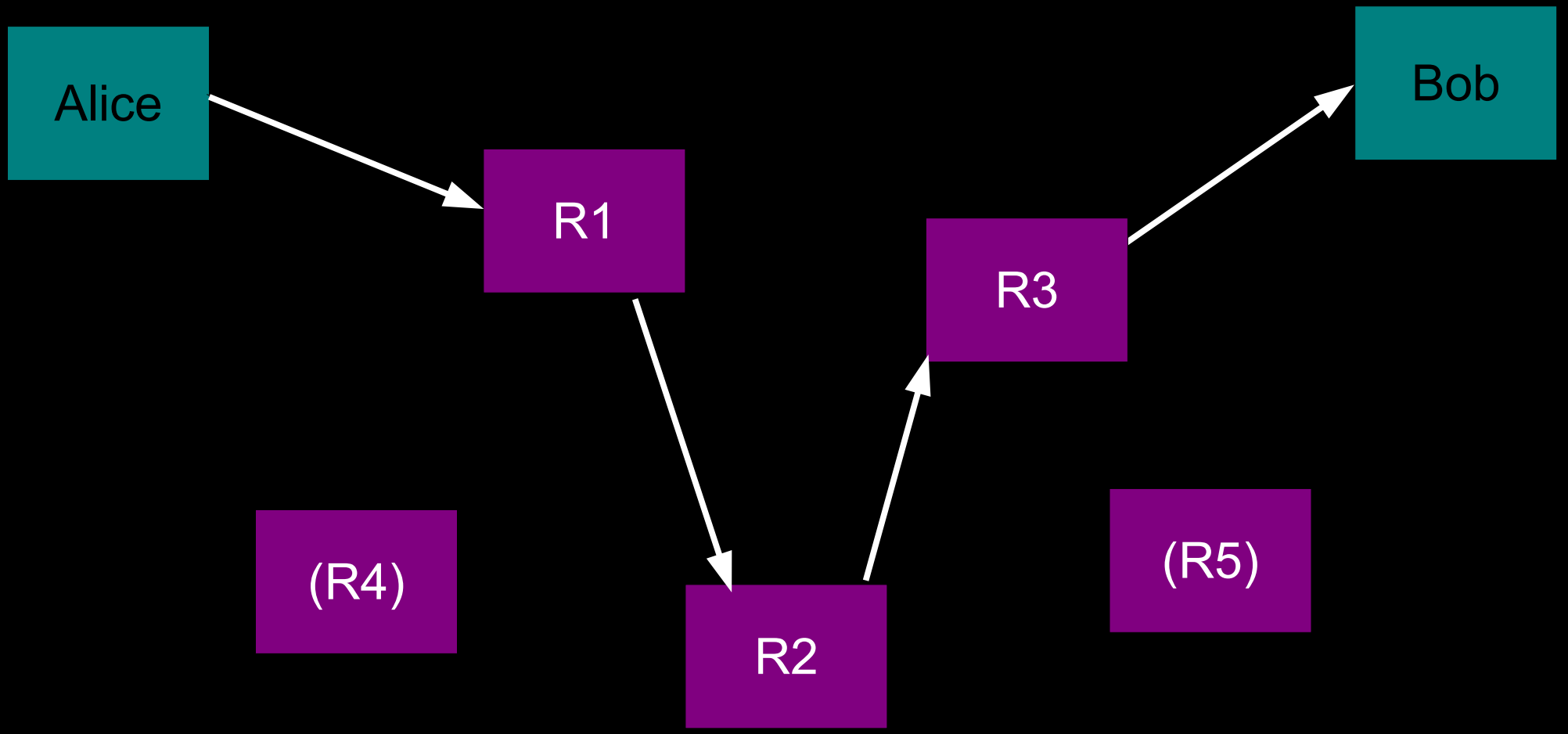
Tor: Verbindungsaufbau

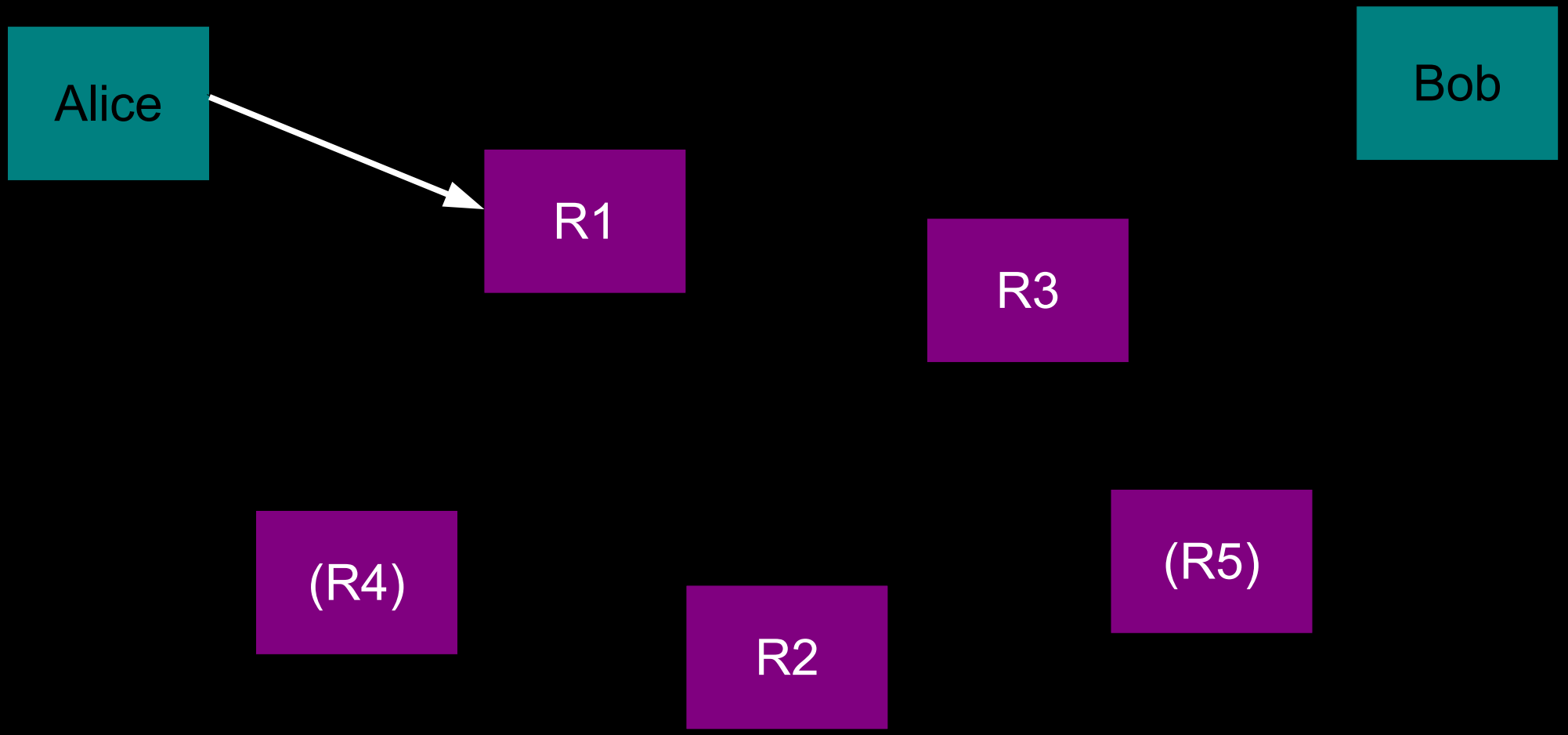


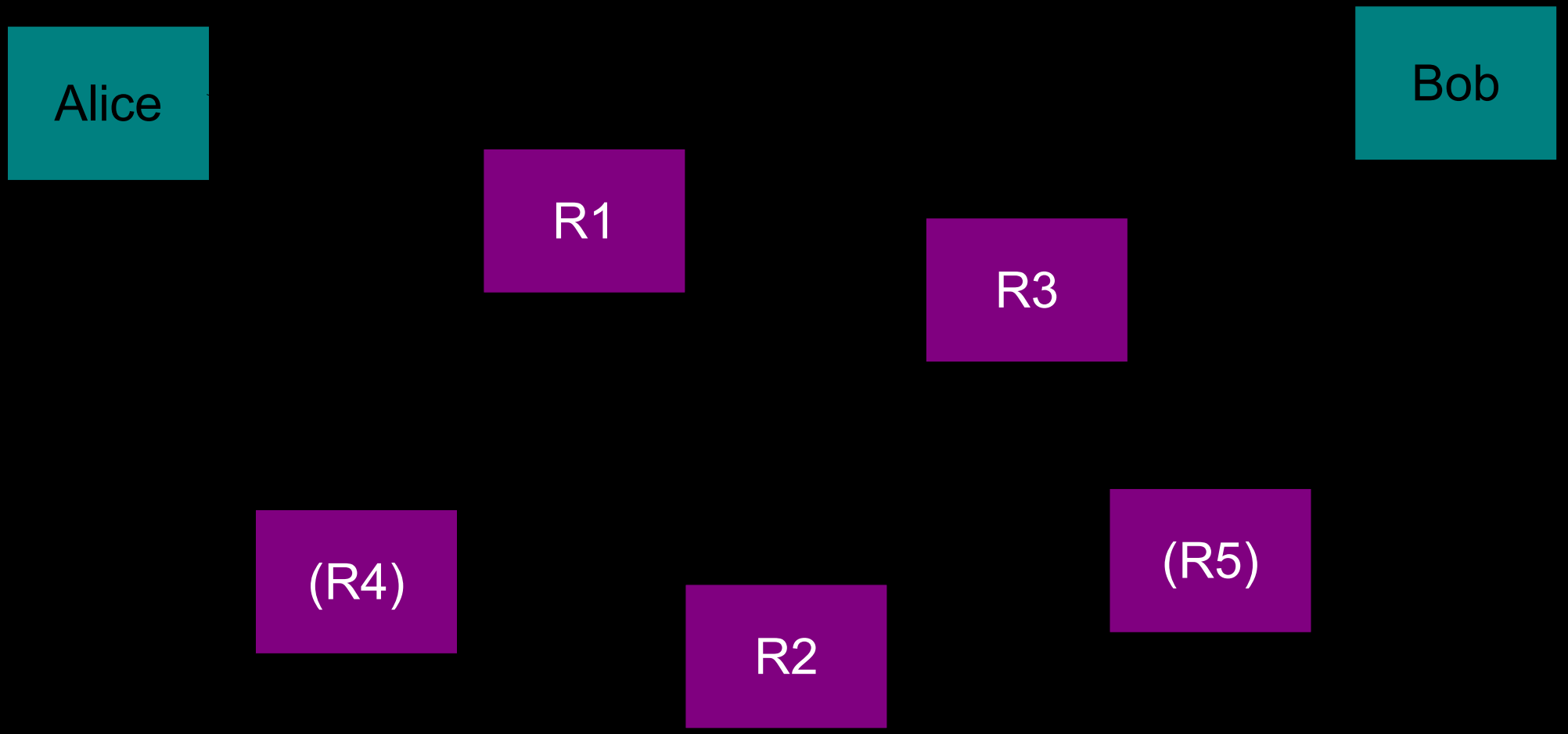
Tor: Verbindungsaufbau

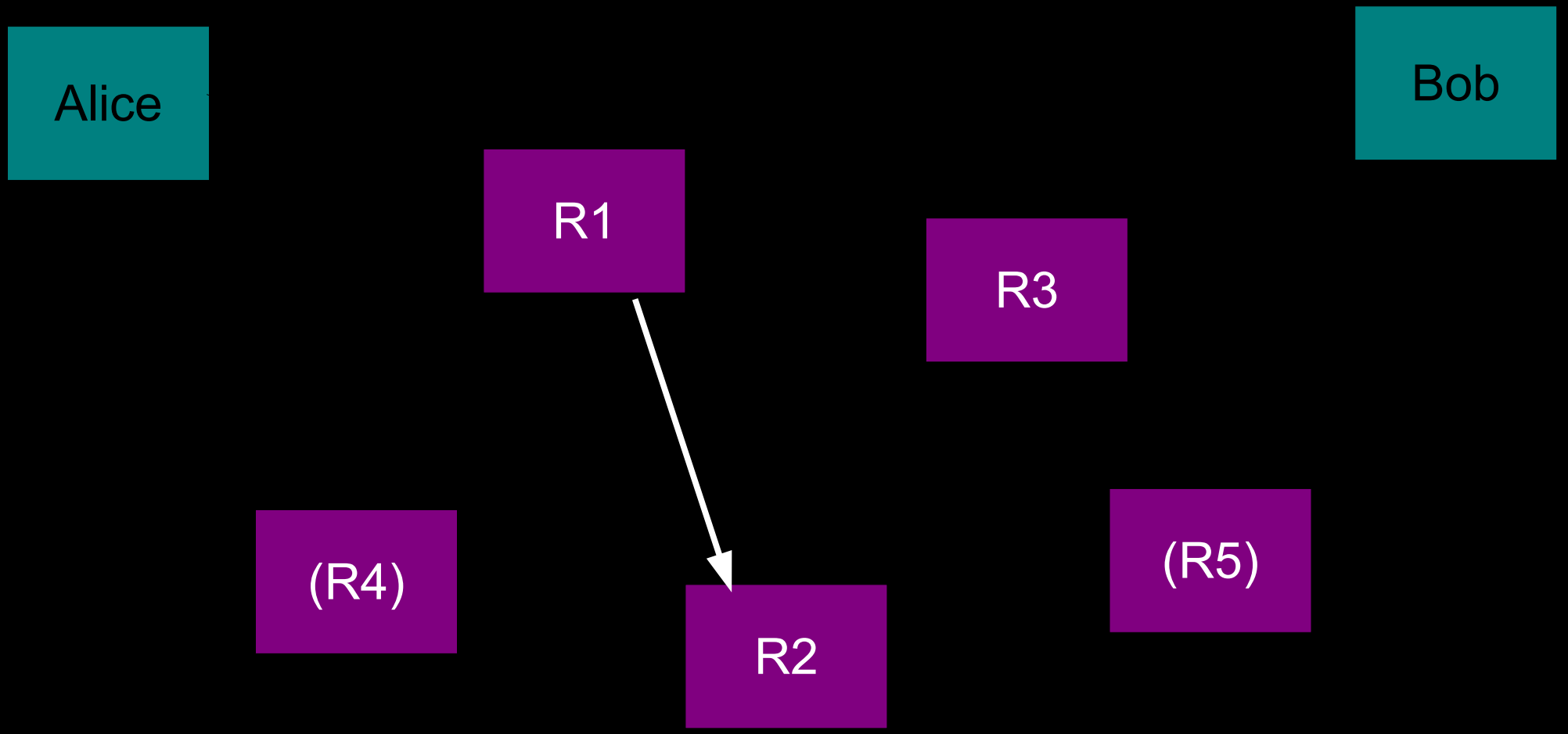


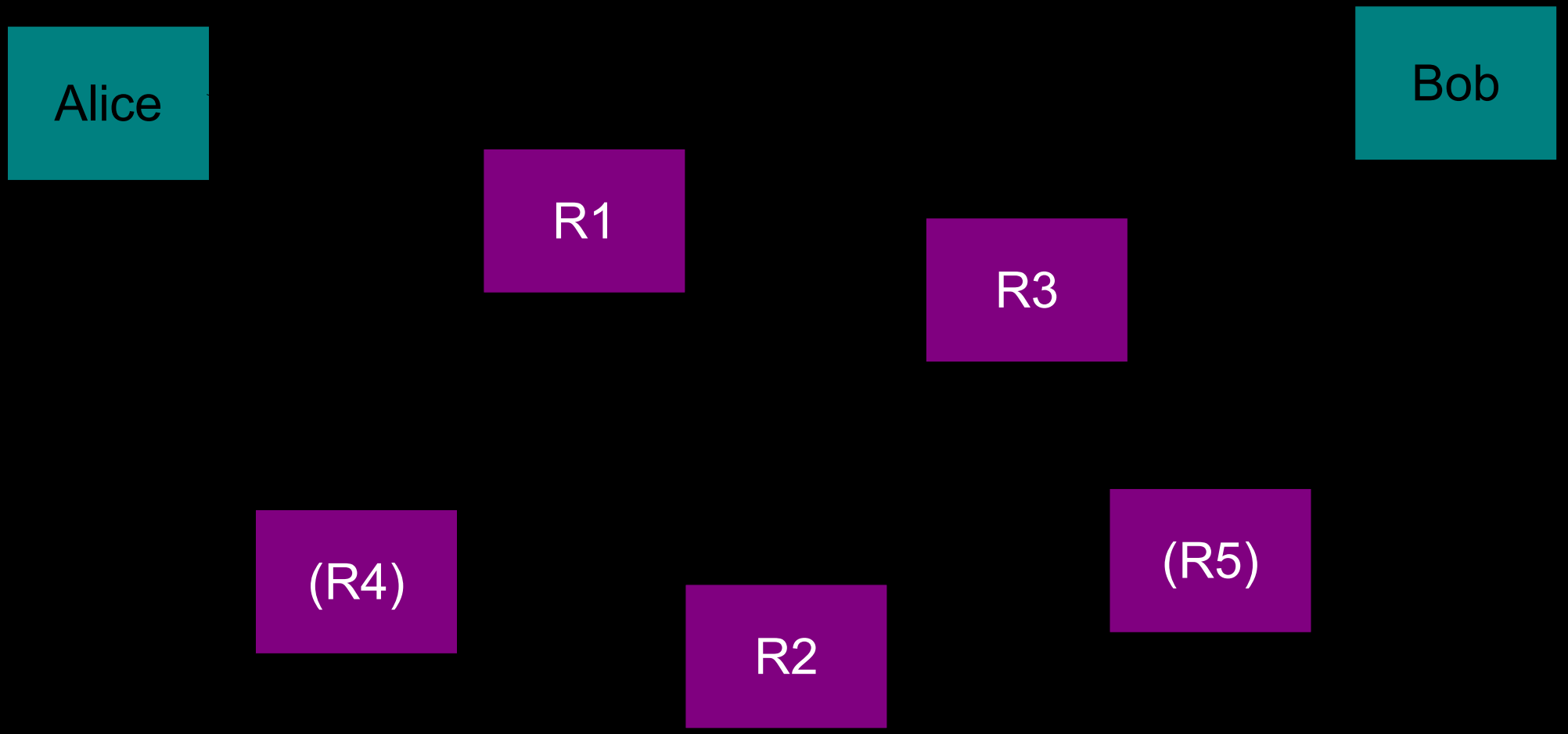
Mixnets: nachrichtenbasiert statt paketbasiert !

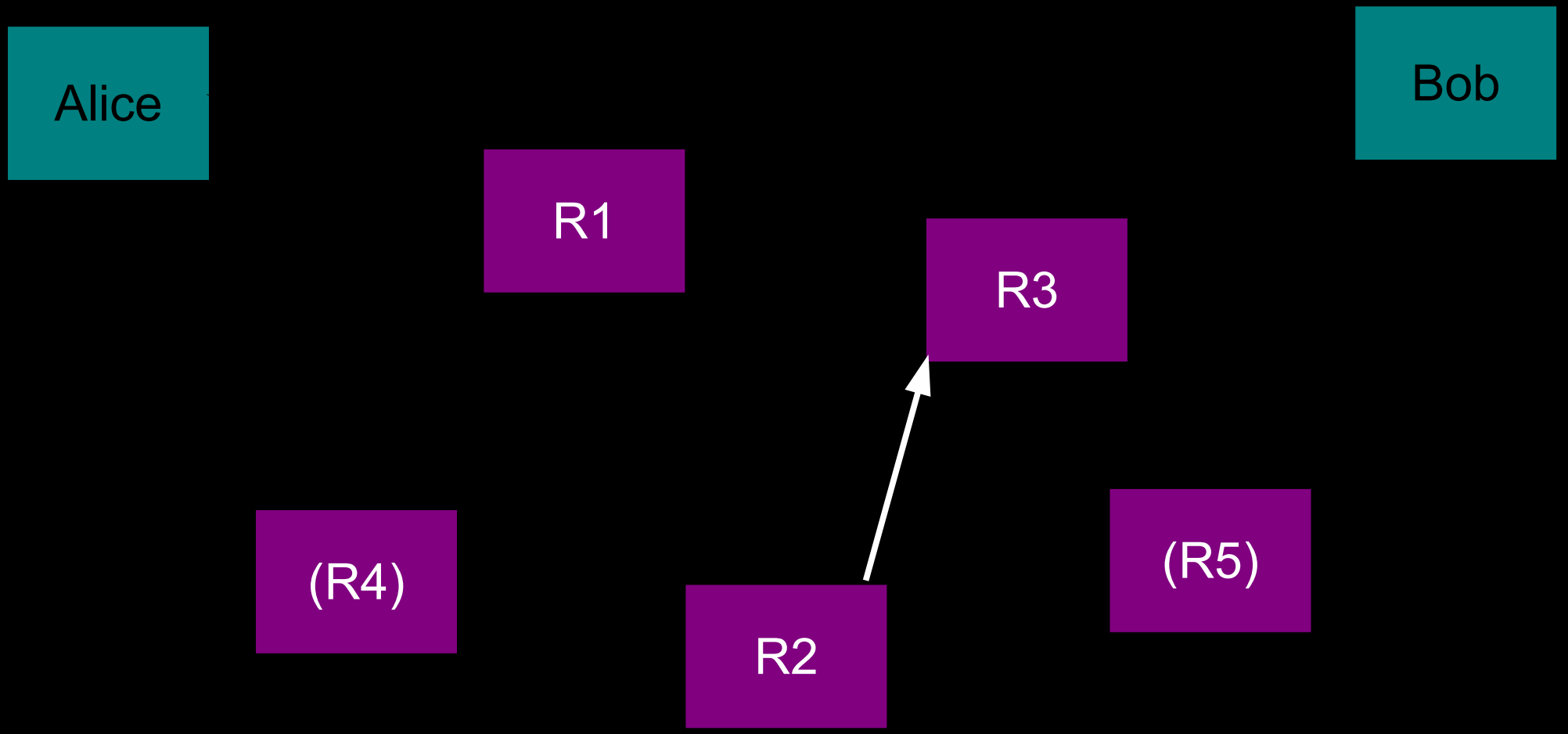


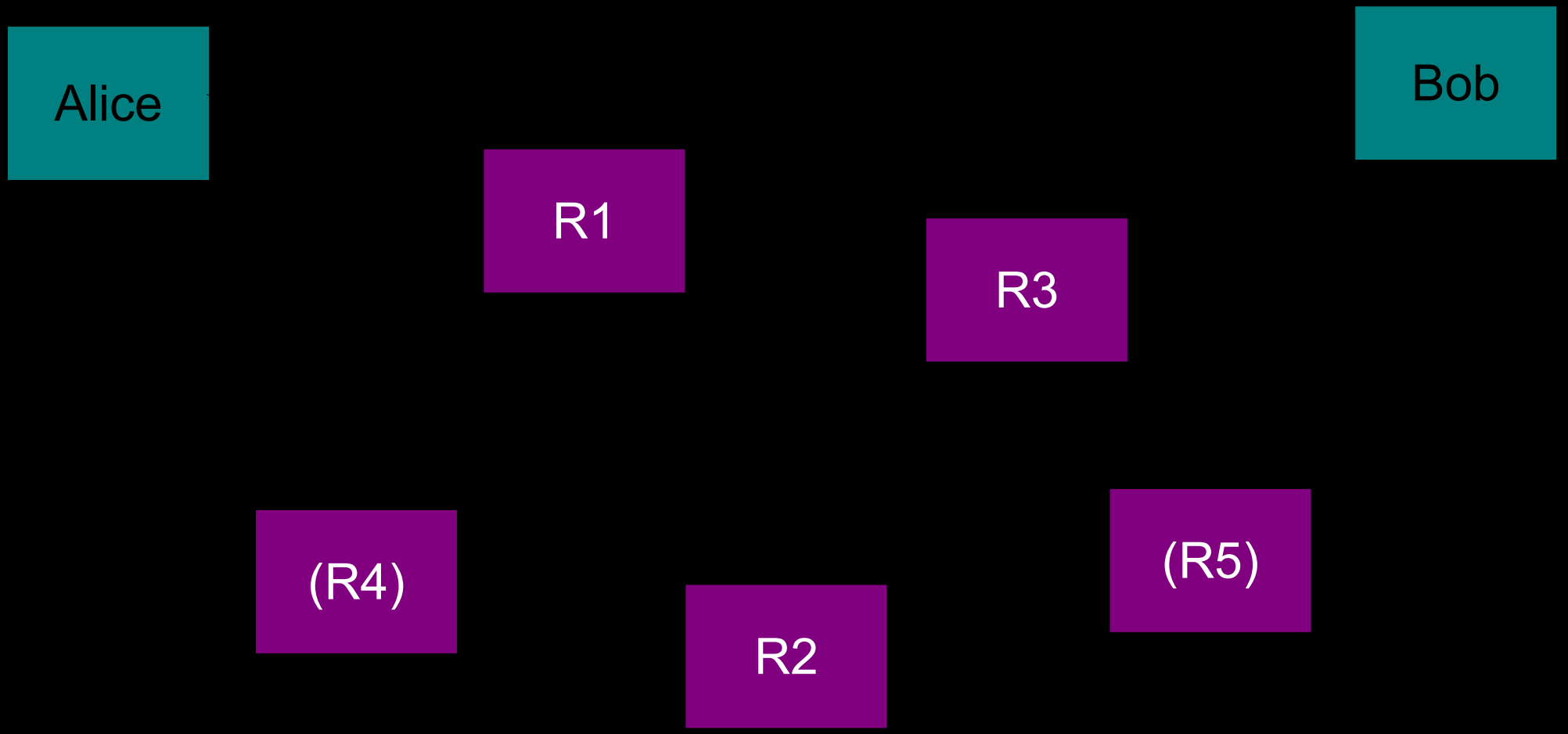

Alice
Bob
R1
R3
(R4)
R2
(R5)

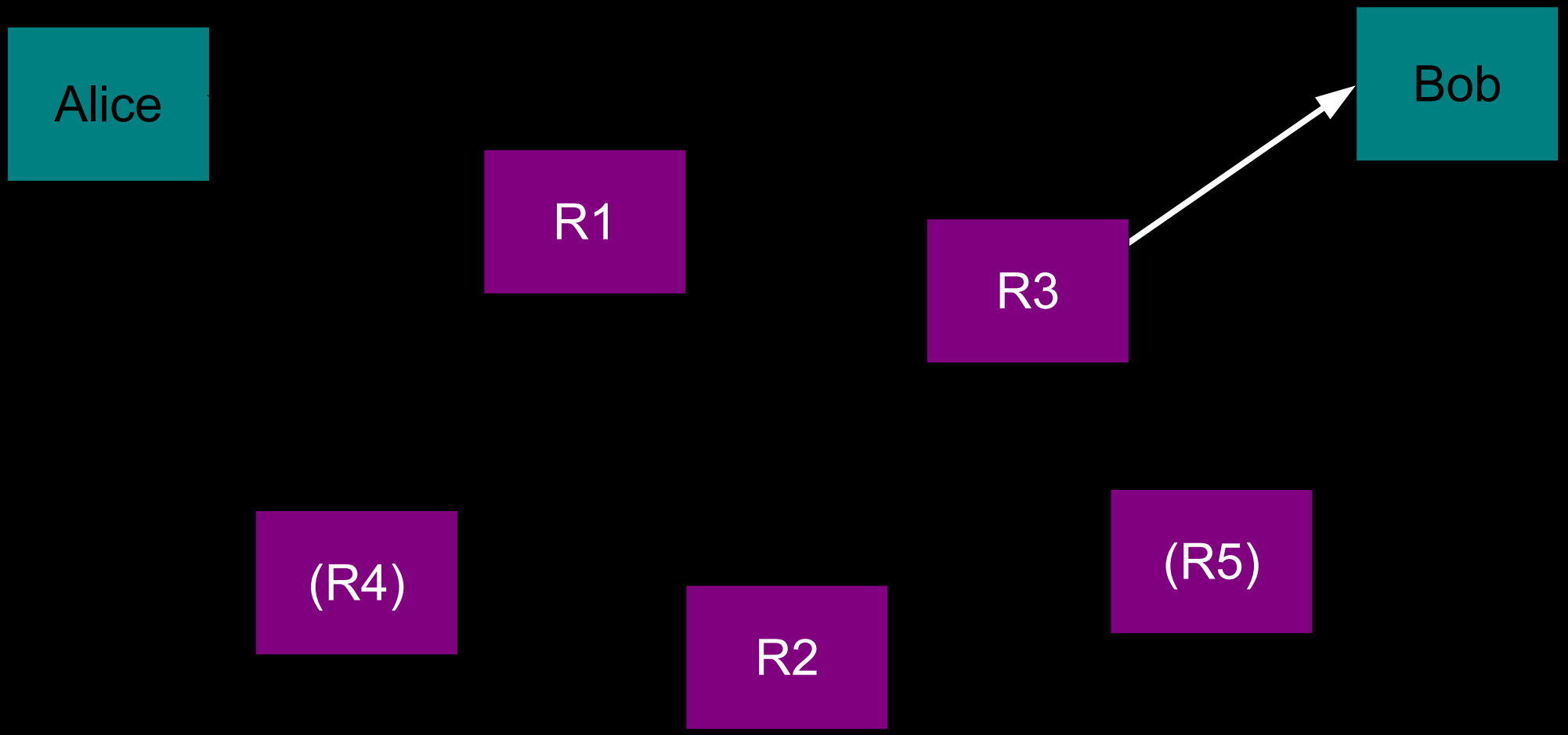

Alice
Bob
R1
R3
(R4)
R2
(R5)


Alice
Bob
R1
R3
(R4)
(R5)
R2


Alice
Bob
R1
R3
(R4)
R2
(R5)


Alice
Bob
R1
R3
(R4)
(R5)
R2


Alice
Bob
R1
R3
(R4)
R2
(R5)


Alice
R1
R3
Bob
(R4)
R2
(R5)

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

Mixing

- Wenige und dafür schnelle Relays ausreichend und sinnvoller
  - Gute Skalierung
  - Dummy Traffic einfacher, zumindest innerhalb des Netzes (“Ränder” → Client-Bandbreite, Energieverbrauch)

- 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

https://bib.mixnetworks.org/

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

- Basierend auf Loopix
- Ursprüngliches Design: Relationship Anonymity (“Traffic analysis resistance”)
- https://katzenpost.mixnetworks.org/
  - Go, Rust

Katzenpost

- Basierend auf Loopix
- Ursprüngliches Design: Relationship Anonymity (“Traffic analysis resistance”)
- https://katzenpost.mixnetworks.org/
  - Go, Rust

→ **https://lists.mixnetworks.org/**

Bootstrapping

- “Zentrale” Authorities vs. “peer2peer”-Modell

Die Zukunft im Solarpunk

- Tree Area Networks
- Steganographie
- DTNs: Delay/Disruption Tolerant Networking
  - Briar
- No Tech Magazine / Low Tech Magazine

Bonus Materialz

Objective

Design an infrastructure that

- **Makes traffic analysis hard**
- **Separates identification from routing**
- **Is reusable across many applications**

Our goal is *anonymous connections*, not anonymous communication.

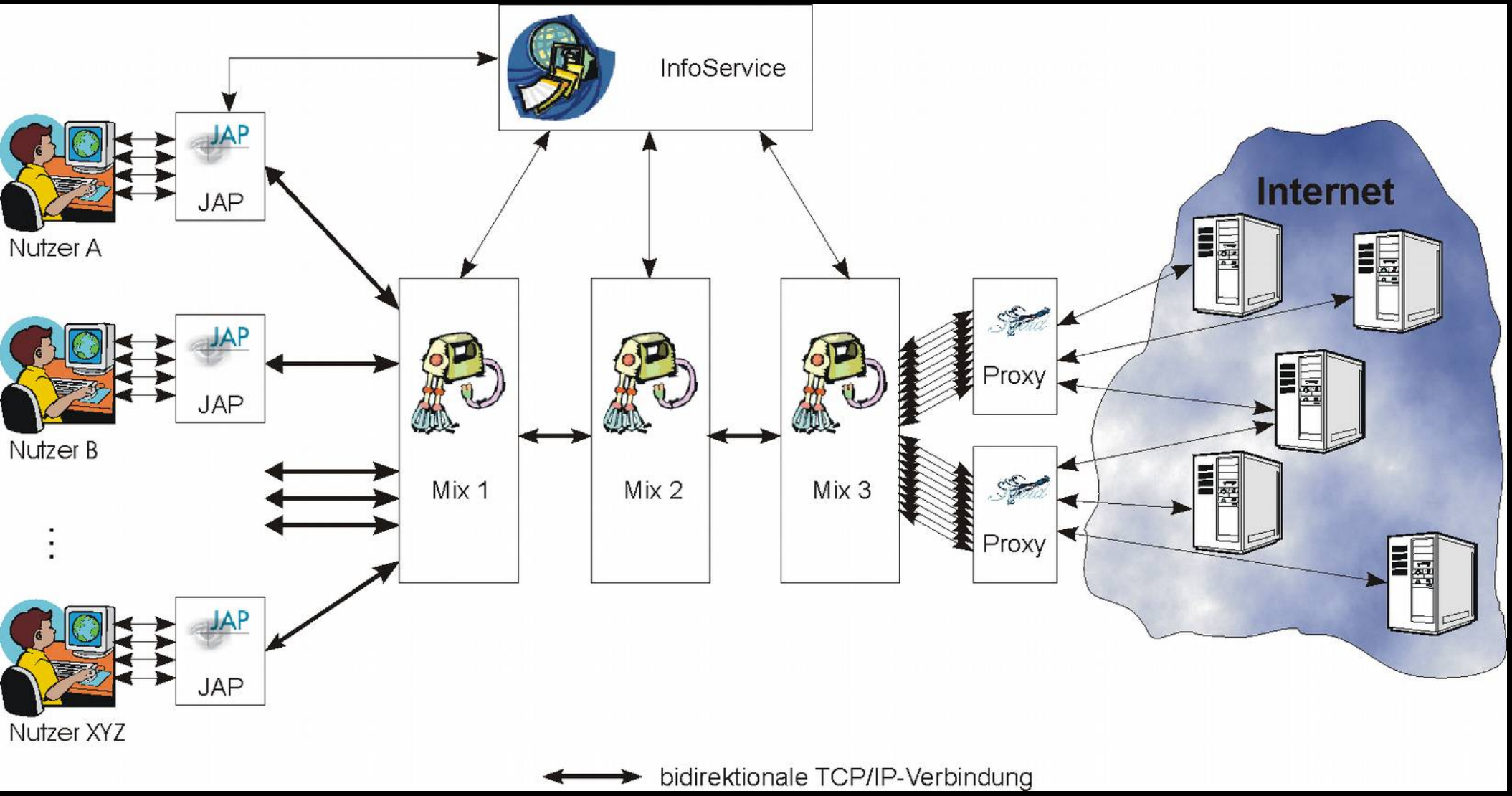
An infrastructure, *Onion Routing*, has been implemented.

Goldschlag, Reed, Syverson: Naval Research Laboratory Briefing 1996
http://www.onion-router.net/Publications/IH-1996.pdf

Threat Model: Active and Passive Attacks

- All traffic is visible
- All traffic can be modified
- Onion Routers may be compromised
- Compromised Onion Routers may cooperate
- Timing coincidences

Goldschlag, Reed, Syverson: Naval Research Laboratory Briefing 1996
http://www.onion-router.net/Publications/IH-1996.pdf



(from: “JAP Inside”, Stephan Köpsell, 2002
https://anon.inf.tu-dresden.de/develop/anon.ppt)

P R E S S E M I T T E I L U N G (27. August 2003)

Erster Teilerfolg für AN.ON

Das Landgericht Frankfurt am Main hat am gestrigen Tage angeordnet (Az.: 5/6 Qs 47/03), dass die Vollziehung des vor einigen Wochen gegenüber den Partnern des AN.ON-Projektes auf Antrag des Bundeskriminalamtes erlassenen richterlichen Beschlusses des Amtsgerichts Frankfurt auszusetzen ist. Nach diesem Beschluss hatte AN.ON, das gemeinsame Projekt des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein und der Technischen Universität Dresden für anonymes Surfen im Internet, den Zugriff auf eine bestimmte IP-Nummer zu protokollieren.

Die Projektpartner haben unmittelbar nach Kenntnis des Beschlusses die auf Grund der ersten richterlichen Anordnung aktivierte Protokollierungsfunktion wieder abgeschaltet. Bis zu diesem Zeitpunkt war ein einziger Datensatz mitprotokolliert worden. Über die Verwendung dieses Protokolldatensatzes wird nach der endgültigen Entscheidung des Landgerichtes zu entscheiden sein. Er befindet sich derzeit in der Obhut des AN.ON-Projektes.

Die Projektpartner werden nach der Entscheidung des Landgerichts eine ausführliche Dokumentation über den Hergang des Verfahrens veröffentlichen.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstr. 98, 24103 Kiel
Tel.: 0431/988-1200
Fax: 0431/988-1223
E-Mail: **mail@datenschutzzentrum.de**
Homepage: www.datenschutzzentrum.de

P R E S S E M I T T E I L U N G (2. September 2003)

BKA geht gegen Anonymitätsdienst vor

Das Bundeskriminalamt (BKA) hat am vergangenen Freitag einen erneuten richterlichen Beschluss gegen das AN.ON-Projekt erwirkt. Mit diesem Beschluss des Amtsgerichts Frankfurt am Main wurde die Durchsuchung der Räume des AN.ON-Projektes an der Technischen Universität Dresden (TU) angeordnet, um für polizeiliche Ermittlungen einen Protokolldatensatz aufzufinden, der auf der Grundlage einer zwischenzeitlich außer Vollzug gesetzten richterlichen Anordnung aufgezeichnet worden war. Am Samstag suchten Beamte des BKA die häusliche Wohnung des Direktors des Instituts für Systemarchitektur an der Fakultät Informatik auf und verlangten von ihm die Herausgabe des Protokolldatensatzes. Da nur auf diese Weise eine Durchsuchung des Instituts durch die Polizeibeamten und damit größerer Schaden für die TU Dresden abgewendet werden konnte, wurde der Datensatz herausgegeben. Nach Auffassung der Betreiber von AN.ON ist dieses Vorgehen des BKA vom Gesetz nicht gedeckt.

Der Beschluss des Amtsgerichtes ist nach Auffassung der Projektpartner rechtswidrig. Da die Vollziehung der in einem vorangegangenen Beschluss des Amtsgerichts angeordneten Auskunftsverpflichtung (gem. §§ 100 g, h StPO) vom Landgericht Frankfurt am Main ausgesetzt worden war, war klargestellt, dass bis zur Entscheidung in der Hauptsache keine Herausgabepflicht für AN.ON bestand. Deshalb ist es eine rechtsmissbräuchliche Umgehung dieser Entscheidung des Landgerichts, die Herausgabe des Protokolldatensatzes mit Hilfe eines neuen Durchsuchungsbeschlusses des Amtsgerichtes zu erzwingen. Nachdem das Landgericht vorläufig zugunsten von AN.ON entschieden hatte, durfte das BKA nicht, wie hier geschehen, auf allgemeine Herausgabe- und Beschlagnahmebestimmungen (§§ 103, 105 StPO) ausweichen. Die Projektpartner werden auch gegen diesen Beschluss durch Einlegung von Rechtsmitteln vorgehen. Eine gerichtliche Überprüfung des Vorgehens der Beamten des BKA halten die Projektpartner für zwingend erforderlich.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstr. 98, 24103 Kiel
Tel.: 0431/988-1200
Fax: 0431/988-1223
E-Mail: **mail@datenschutzzentrum.de**
Homepage: www.datenschutzzentrum.de

P R E S S E M I T T E I L U N G (04. November 2003)

AN.ON erneut gegen Bundeskriminalamt erfolgreich

Das Landgericht Frankfurt (5/8 Qs 26/03) hat nun auch in der dritten gerichtlichen Auseinandersetzung zwischen dem BKA und den Betreibern des Anonymisierungsdienstes AN.ON zugunsten von AN.ON entschieden. Ebenso wie bei den beiden vorangegangenen Entscheidungen einer anderen Kammer des LG Frankfurt (Az.: 5/6 Qs 47/03) wurde die Rechtsauffassung von AN.ON bestätigt.

Auf die Beschwerde der Projektbetreiber stellte das Gericht die Rechtswidrigkeit der vom Amtsgericht Frankfurt am 29. August 2003 gegen das Projekt erlassenen Durchsuchungsanordnung für die Räume des AN.ON-Projektes an der Technischen Universität (TU) Dresden fest. Damit ist klargestellt, dass das Vorgehen der BKA-Beamten, die im August auf der Herausgabe eines - auf Grund eines ebenfalls rechtswidrigen richterlichen Beschlusses - gespeicherten Protokolldatensatzes bestanden hatten, vom Gesetz nicht gedeckt war.

Die Projektpartner hatten in ihrer Beschwerde die Auffassung vertreten, die Durchsuchungsanordnung stelle eine rechtsmissbräuchliche Umgehung des Beschlusses des Landgerichts dar, mit dem die Vollziehung der Auskunftsverpflichtung ausgesetzt worden war. Das Landgericht folgte dieser Argumentation, indem es feststellte, dass die Durchsuchungsanordnung eine Umgehung der §§ 100g, h StPO darstelle. Es führte wörtlich aus: "die Normen des §§ 100g, h StPO verdrängen die Möglichkeit, im Wege der Beschlagnahme bei einer Durchsuchung solche Daten zu Informationszwecken zu erlangen, bezüglich derer das Vorliegen einer Auskunftserteilungpflicht nach § 100g StPO zu prüfen wäre."

Nachdem die Projektpartner mit allen Rechtsmitteln gegen die Ermittlungshandlungen des BKA erfolgreich waren, sehen sie sich in ihrer Absicht bestärkt, den Nutzern des AN.ON-Dienstes ein wirksames technisches Instrument an die Hand zu geben, das sich vollständig auf dem Boden des Rechts bewegt. Die Entscheidungen der 6. und 8. Kammer des Landgerichts Frankfurt zeigen, dass das Vorgehen des BKA gegen AN.ON auch nach Auffassung der Gerichte nicht im Einklang mit der Strafprozessordnung stand.

Die Projektbetreiber haben nunmehr das BKA und die Staatsanwaltschaft Frankfurt am Main aufgefordert, den fraglichen Protokolldatensatz zurückzugeben und seine Löschung in den polizeilichen Datensammlungen zu bestätigen. Gleichzeitig haben die Projektpartner den zuständigen Bundesbeauftragten für den Datenschutz sowie den Hessischen Datenschutzbeauftragten gebeten, die Löschung der Daten zu überprüfen.

Traffic Correlation

"The Java Anon Proxy (also known as JAP or Web MIXes) uses fixed shared routes known as cascades. As with a single-hop proxy, this approach aggregates users into larger anonymity sets, but again an attacker only needs to observe both ends of the cascade to bridge all the system's traffic. The Java Anon Proxy's design calls for padding between end users and the head of the cascade. **However, it is not demonstrated whether the current implementation's padding policy improves anonymity.**" (Tor Design Paper, 2004)

- "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.)
- "Currently nodes are not required to do any sort of link padding or dummy traffic. **Because strong attacks exist even with link padding, and because link padding greatly increases the bandwidth requirements for running a node**, we plan to leave out link padding until this tradeoff is better understood." (Tor Protocol Specification)

Traffic Correlation

The Tor design doesn't try to protect against an attacker who can see or measure both traffic going into the Tor network and also traffic coming out of the Tor network. That's because if you can see both flows, some simple statistics let you decide whether they match up. […]

The way we generally explain it is that Tor tries to protect against traffic analysis, where an attacker tries to learn whom to investigate, but Tor can't protect against traffic confirmation (also known as end-to-end correlation), where an attacker tries to confirm a hypothesis by monitoring the right locations in the network and then doing the math.

And the math is really effective. There are simple packet counting attack and moving window averages, but the more recent stuff is downright scary, like Steven Murdoch's PET 2007 paper about achieving **high confidence in a correlation attack despite seeing only 1 in 2000 packets on each side** (Sampled Traffic Analysis by Internet-Exchange-Level Adversaries).

https://blog.torproject.org/blog/one-cell-enough

(C//REL) Types of IAT – Advanced Open Source Multi-Hop

(S//REL) Open Source Multi-Hop Networks

- (S//REL) *Tor*
- (S//REL) Very widely used worldwide
- (S//REL) Open Source
  - (S//REL) Active Development
  - (S//REL) Mitigates Threats
- (S//REL) Very Secure
- (S//REL) Low enough latency for most *TCP* uses
- (S//REL) Still the King of high secure, low latency Internet Anonymity
  - (S//REL) There are no contenders for the throne in waiting

Stinks (U)

[redacted]

CT SIGDEV

[redacted]

JUN 2012

Tor Stinks... (U)

- We will never be able to de-anonymize all Tor users all the time.
- With manual analysis we can de-anonymize a **very small fraction** of Tor users, however, **no** success de-anonymizing a user in response to a TOPI request/on demand.

UK TOP SECRET STRAP1 COMINT

AUS/CAN/NZ/UK/US EYES ONLY

Reference: OPC-M/TECH.A/455 (v1.0, r206)
Date: 20 September 2011
Copy no:

HIMR Data Mining Research Problem Book

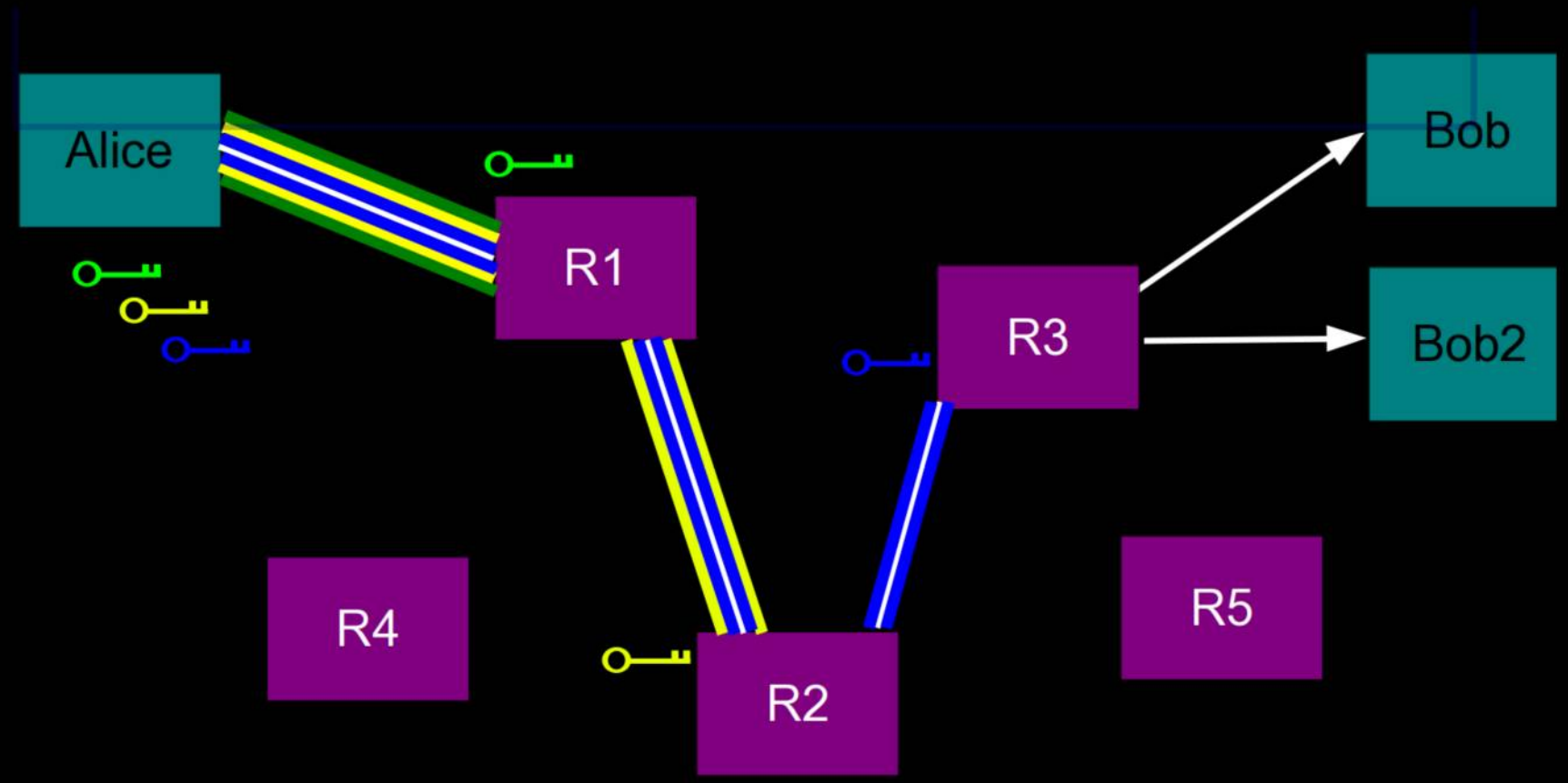
[redacted]

OPC-MCR, GCHQ

ICTR-NE ICTR-NE are interested in using information flows to find Tor routes, identify backhaul routes and map botnets. They currently have a Hadoop prototype called HIDDEN OTTER which performs simple temporal chaining. They would be very interested in any work you produce and may wish to collaborate. HIDDEN OTTER was produced by [redacted] and [redacted]

Who runs the relays?

- “operate” or “surveil”?



The next step

- We are collecting the required logs of packet times with TOR guard nodes in SIGINT
- GTE / JTRIG have adapted some TOR exit nodes we own to collect the required exit node data
  - We are keen to engage with others with exit nodes too
- Then run the attack
  - Expect to basically work
  - Some extra work might be required to only allow queries on sessions with enough structure
    - Need the bulk data first to progress this question

Conclusion

- Have shown a potential externals-based deanonymisation attack for TOR
  - Requires SIGINT collection of guard-to-client packet times
  - Requires TOR collection from exit nodes we own
- Hope to get this running live at GCHQ soon

Reference: OPC-M/TECH.B/61
Date: 13 June 2011
Copy no:

A potential technique to deanonymise users of the TOR network

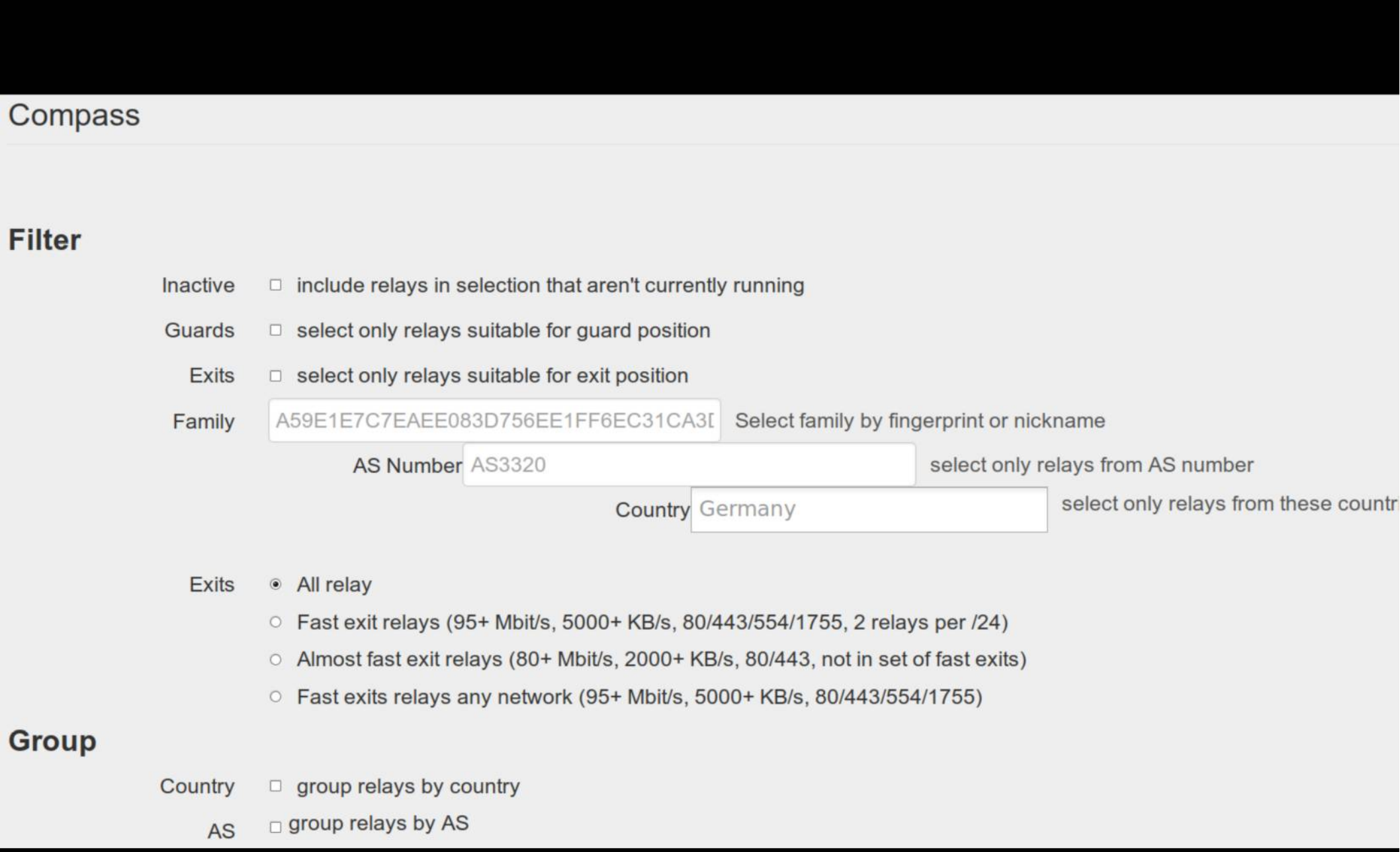
[redacted]
OPC-MCR, GCHQ

Summary

A new technique to deanonymise users of the TOR network is demonstrated. It is shown that the majority of a small truthed set of data can be deanonymised without any false hits anywhere in eight bearer-hours of data.

For this algorithm to be further tested we must run some TOR exit nodes and collect data from these. SIGINT packet logging of guard node traffic is also required.

Demonstration software is available in the form of an R package from [redacted]



https://compass.torproject.org/