Walking Onions: Scaling Anonymity Networks while Protecting Users

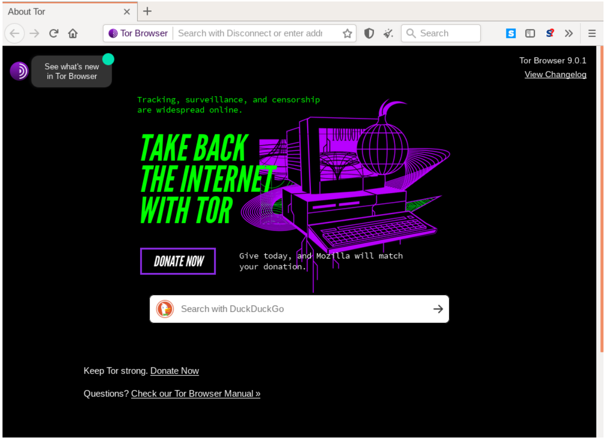
Chelsea H. Komlo[1], Nick Mathewson[2], Ian Goldberg[1]

[1] University of Waterloo [2] The Tor Project

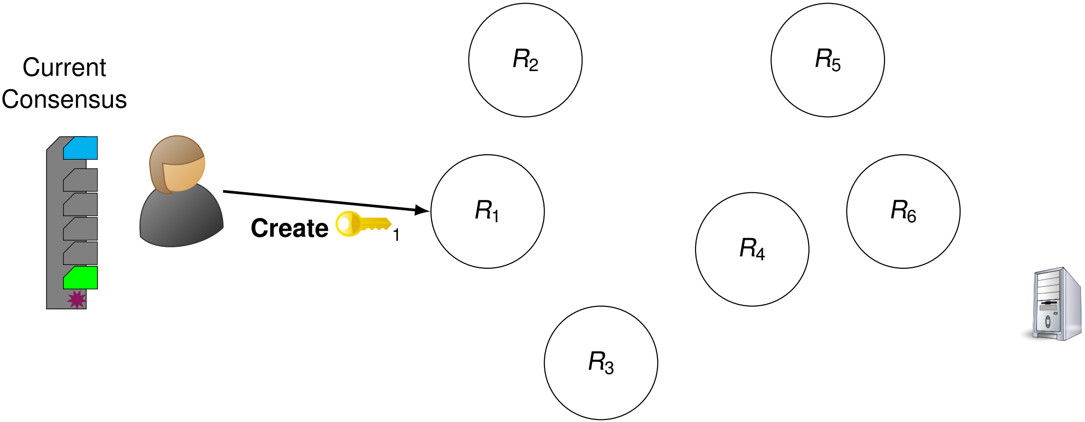
USENIX Security Symposium, 13 August 2020

Cryptography, Security, and Privacy
— Research Group @ uWaterloo —

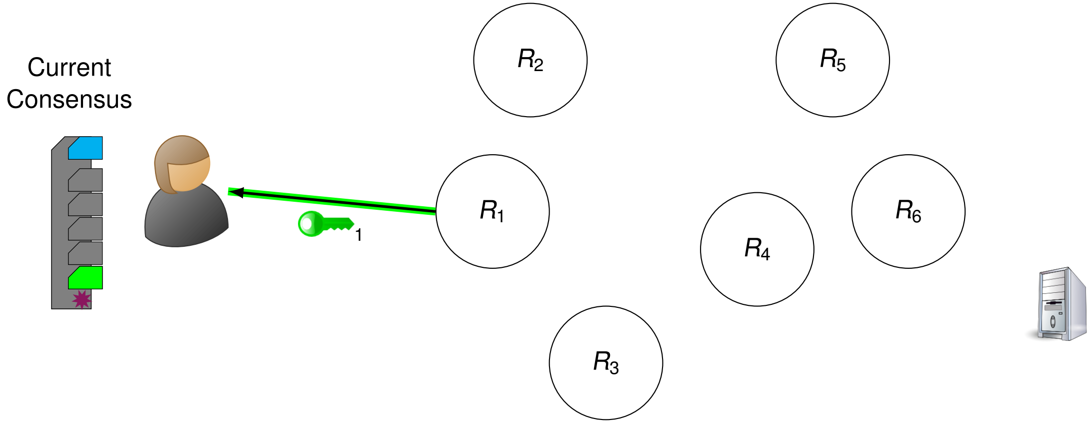
Tor is a privacy-enhancing tool to use the Internet privately and circumvent censorship.



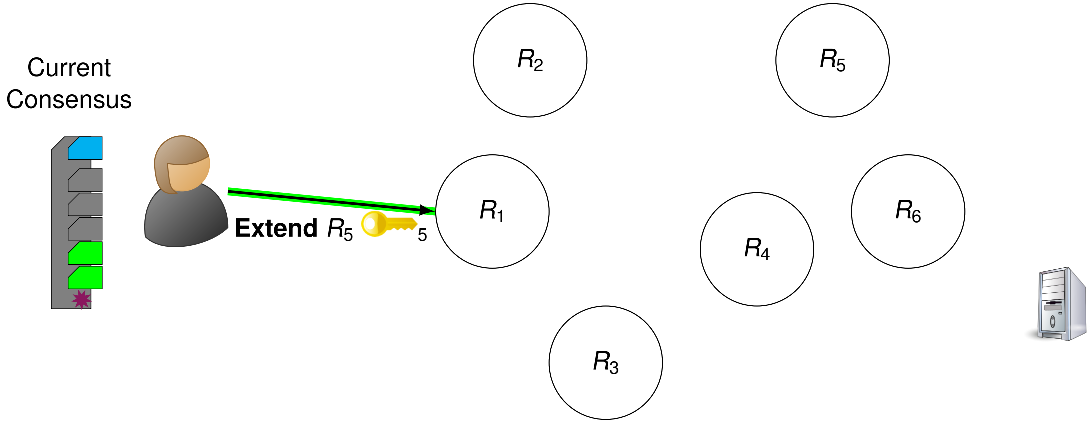
Current Tor Path Selection and Circuit Extension



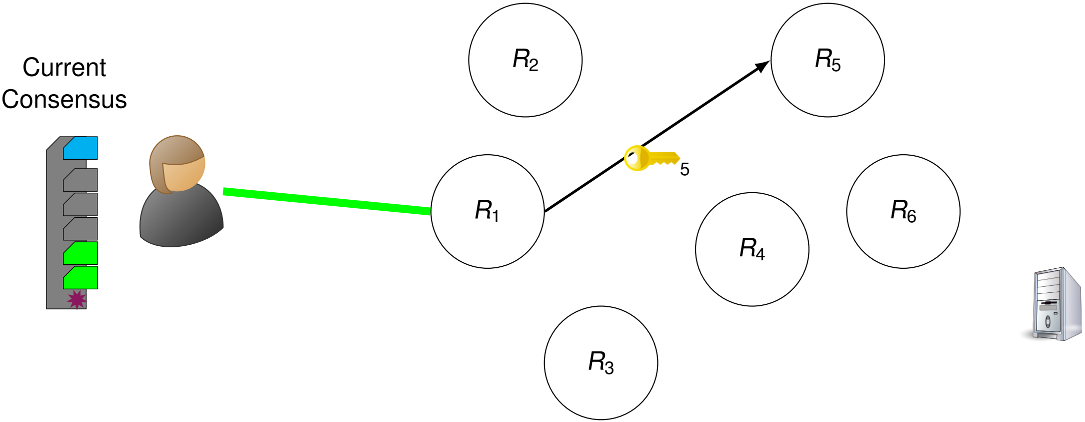
Current Tor Path Selection and Circuit Extension



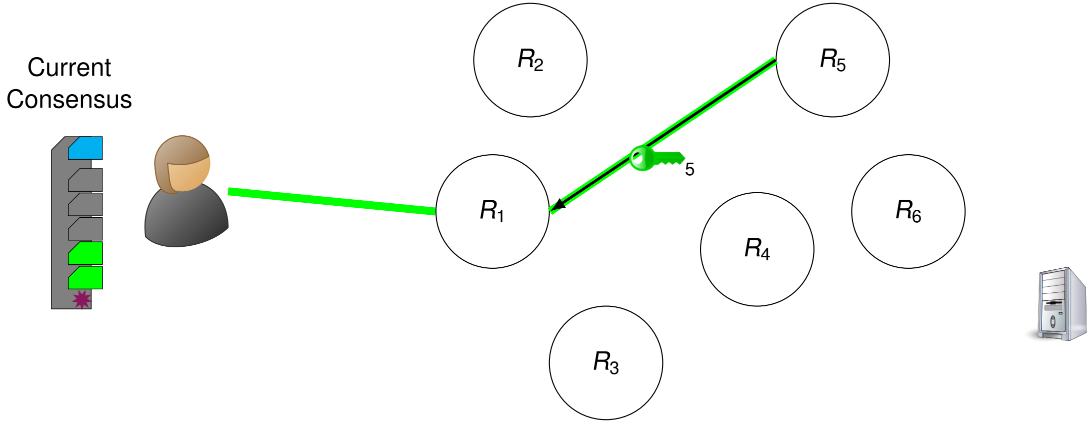
Current Tor Path Selection and Circuit Extension



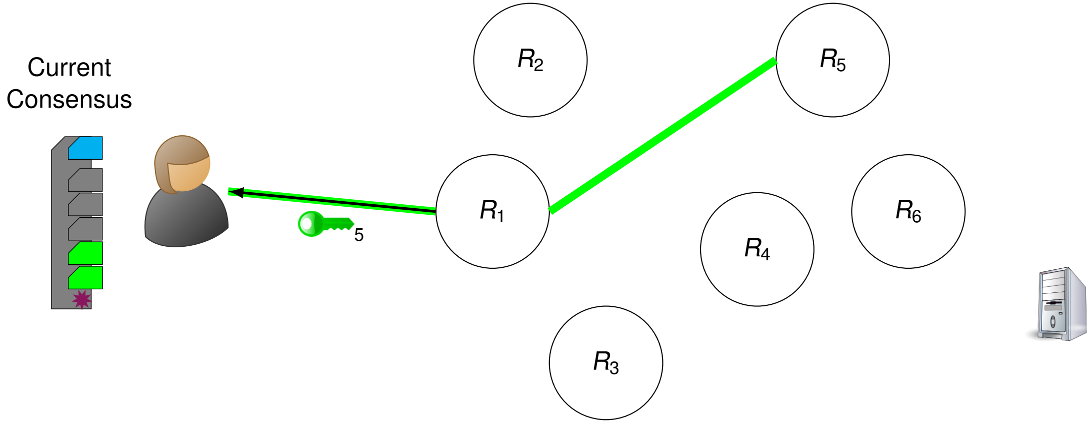
Current Tor Path Selection and Circuit Extension



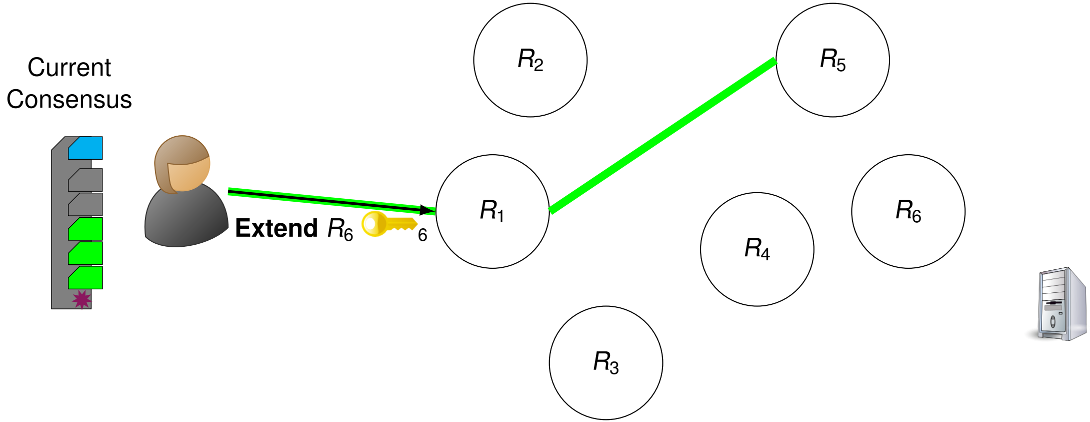
Current Tor Path Selection and Circuit Extension



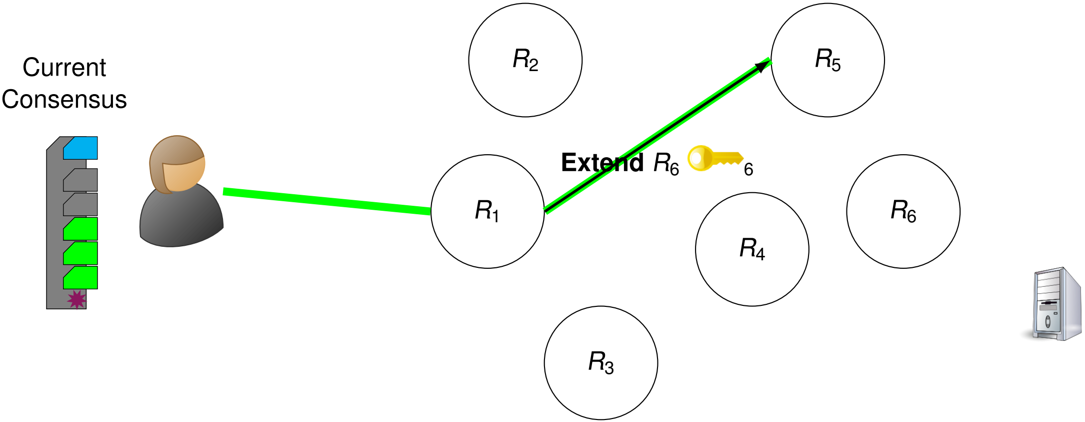
Current Tor Path Selection and Circuit Extension



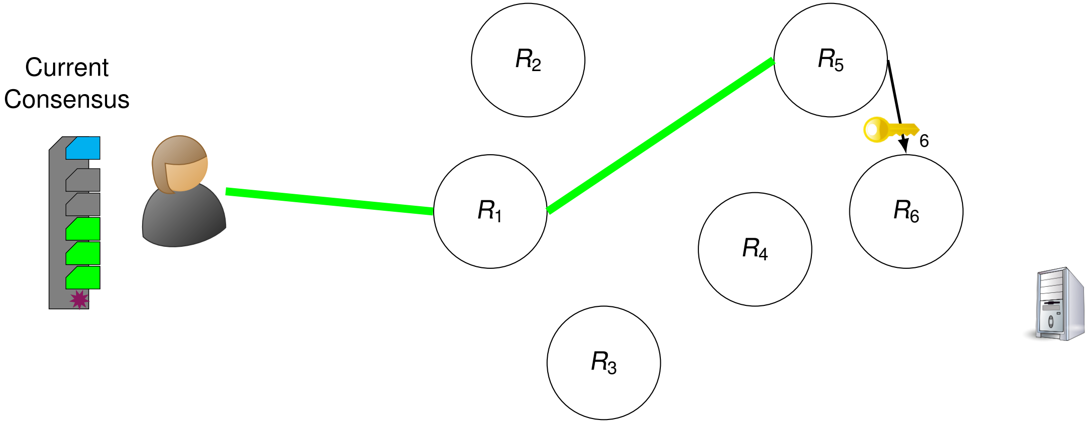
Current Tor Path Selection and Circuit Extension



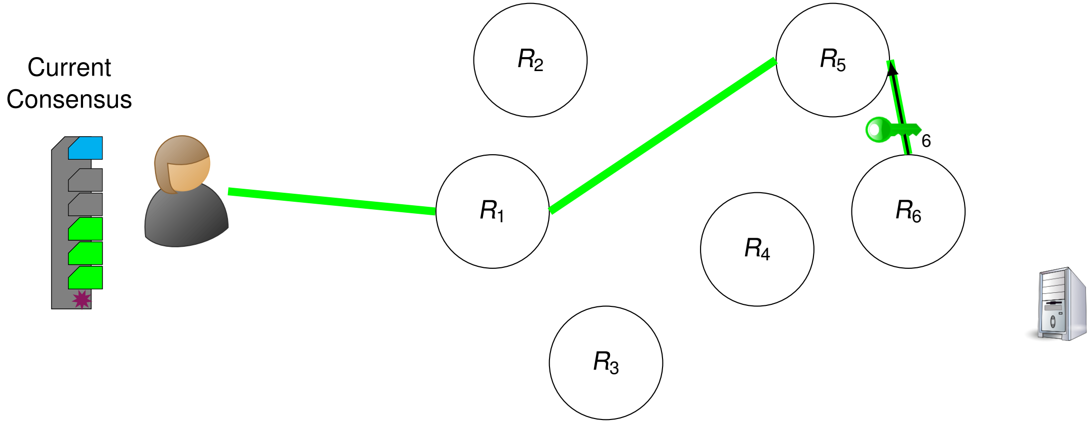
Current Tor Path Selection and Circuit Extension



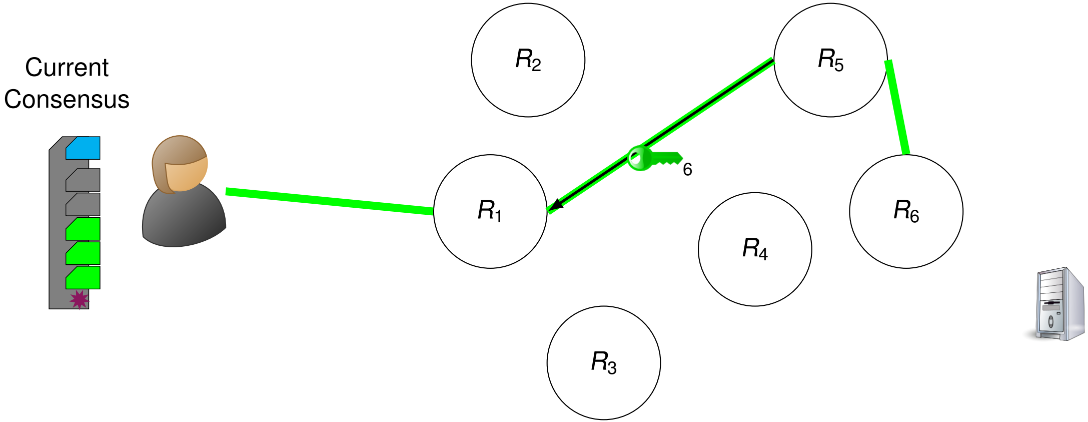
Current Tor Path Selection and Circuit Extension



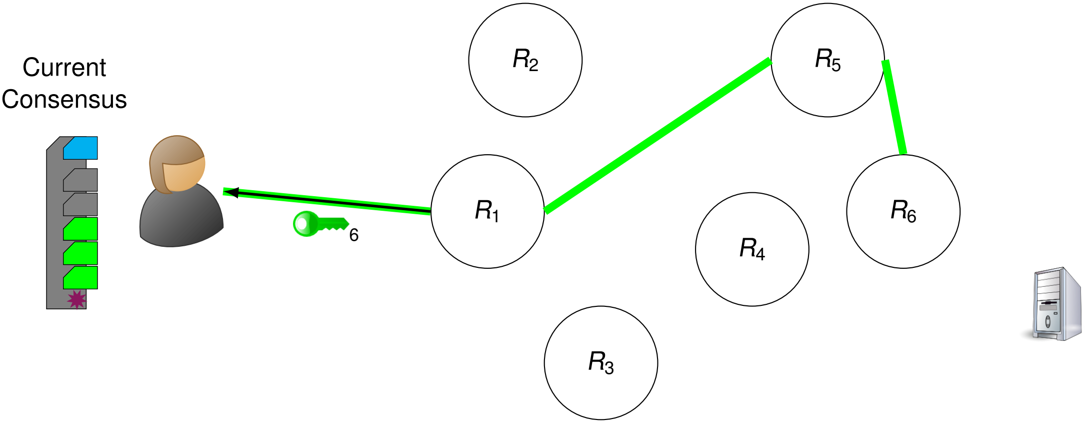
Current Tor Path Selection and Circuit Extension



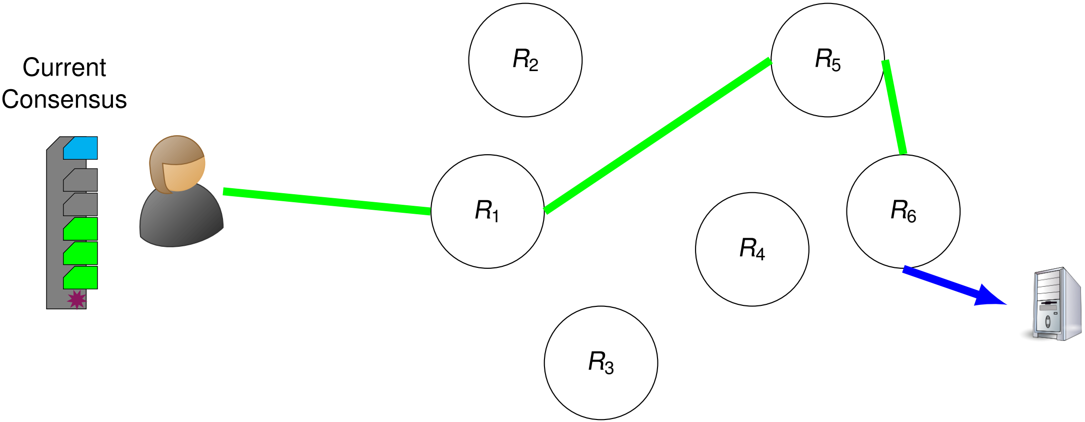
Current Tor Path Selection and Circuit Extension



Current Tor Path Selection and Circuit Extension



Current Tor Path Selection and Circuit Extension



Tor Security Model: Security over Scalability

- **Epistemic Attacks**: Users with different views of the network can be distinguished by their relay selection.

Tor Security Model: Security over Scalability

- **Epistemic Attacks**: Users with different views of the network can be distinguished by their relay selection.

  Tor's Protection: All clients to maintain an up-to-date consensus copy.

Tor Security Model: Security over Scalability

- **Epistemic Attacks**: Users with different views of the network can be distinguished by their relay selection.

  Tor's Protection: All clients to maintain an up-to-date consensus copy.

- **Route-Capture Attacks**: When an adversary can influence users' relay selection.

Tor Security Model: Security over Scalability

- **Epistemic Attacks**: Users with different views of the network can be distinguished by their relay selection.

  Tor's Protection: All clients to maintain an up-to-date consensus copy.

- **Route-Capture Attacks**: When an adversary can influence users' relay selection.

  Tor's Protection: Clients verify relay responses using signing keys in the consensus.

What Contributions Does Walking Onions Make?

- **Constant-Size Client Overhead.** Client bandwidth overhead remains constant even as new relays join (or at worst logarithmic).

What Contributions Does Walking Onions Make?

- **Constant-Size Client Overhead.** Client bandwidth overhead remains constant even as new relays join (or at worst logarithmic).
- **Maintains Tor's Existing Security Model.** One variant has no change, the other a slight loosening of forward secrecy (for path selection, not content).

What Contributions Does Walking Onions Make?

- **Constant-Size Client Overhead.** Client bandwidth overhead remains constant even as new relays join (or at worst logarithmic).
- **Maintains Tor's Existing Security Model.** One variant has no change, the other a slight loosening of forward secrecy (for path selection, not content).
- **Immediate Performance Improvements.** Demonstrates improvements at networks the size of Tor today.

What Contributions Does Walking Onions Make?

- **Constant-Size Client Overhead.** Client bandwidth overhead remains constant even as new relays join (or at worst logarithmic).
- **Maintains Tor's Existing Security Model.** One variant has no change, the other a slight loosening of forward secrecy (for path selection, not content).
- **Immediate Performance Improvements.** Demonstrates improvements at networks the size of Tor today.
- **Generally Applicable.** Aspects of Walking Onions apply to network designs beyond Tor.

What Improvements Does Walking Onions Make?

- How to represent relay information to enable oblivious selection and individual verification?

What Improvements Does Walking Onions Make?

- How to represent relay information to enable oblivious selection and individual verification?
- How to build paths using oblivious relay selection?

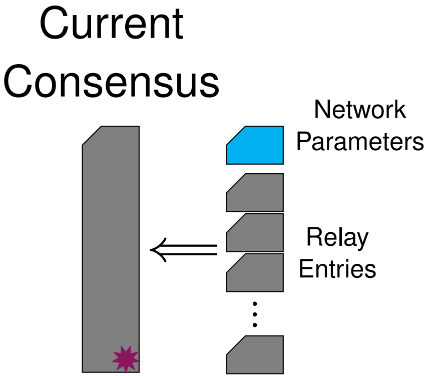
What Improvements Does Walking Onions Make?

- How to represent relay information to enable oblivious selection and individual verification?
- How to build paths using oblivious relay selection?
- How to perform more efficient circuit construction?

What improvements does Walking Onions make?

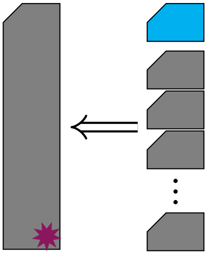
- **How to represent relay information to enable oblivious selection and individual verification?**

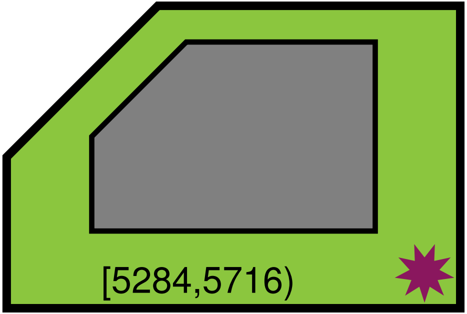
New Data Structure: Seperable Network Index Proof (SNIP)



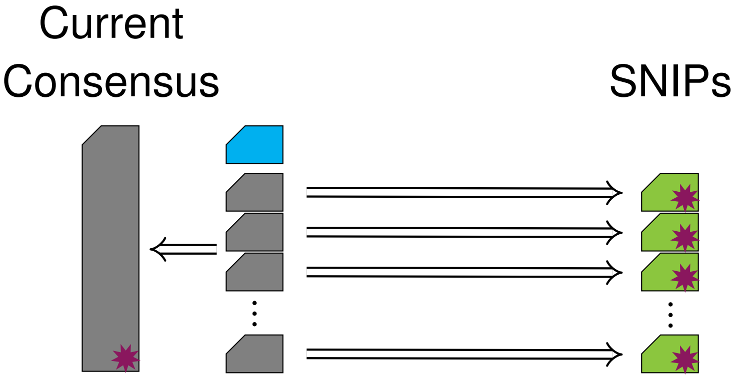
New Data Structure: Seperable Network Index Proof (SNIP)

Current Consensus

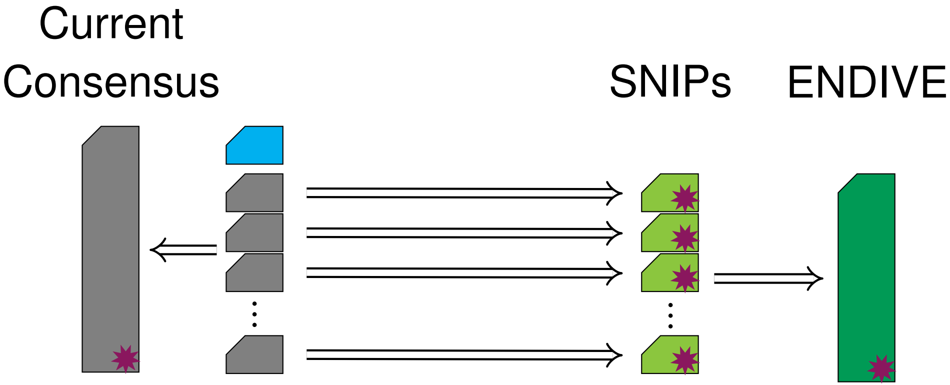




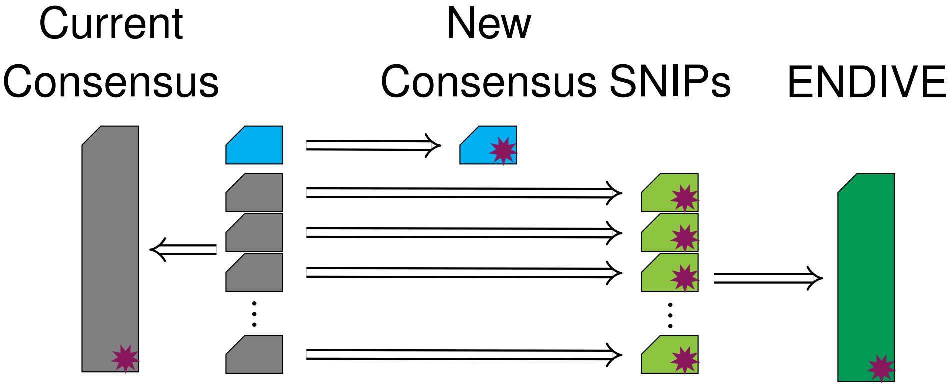
New Data Structure: Seperable Network Index Proof (SNIP)



ENDIVE: Efficient Network Directory with Independently Verifiable Entries



ENDIVE: Efficient Network Directory with Independently Verifiable Entries

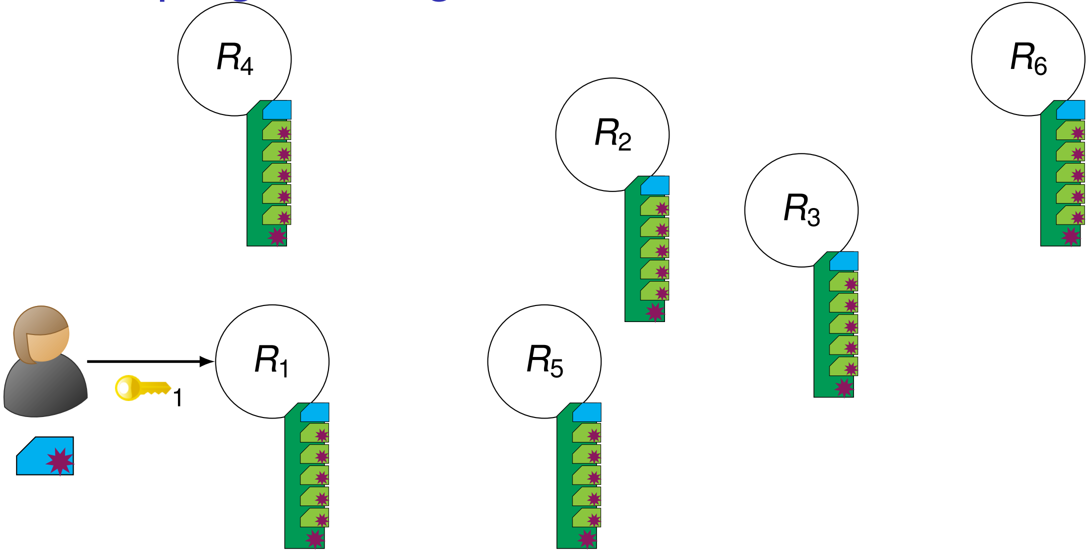


What improvements does Walking Onions make?

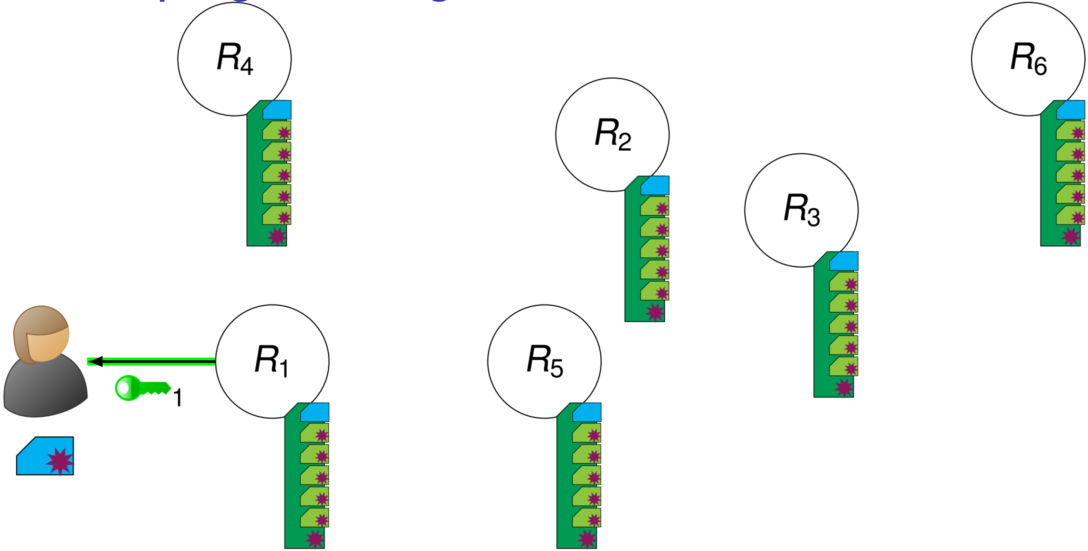
- How to represent relay information to enable oblivious selection and individual verification?

- **How to build paths using oblivious relay selection?**

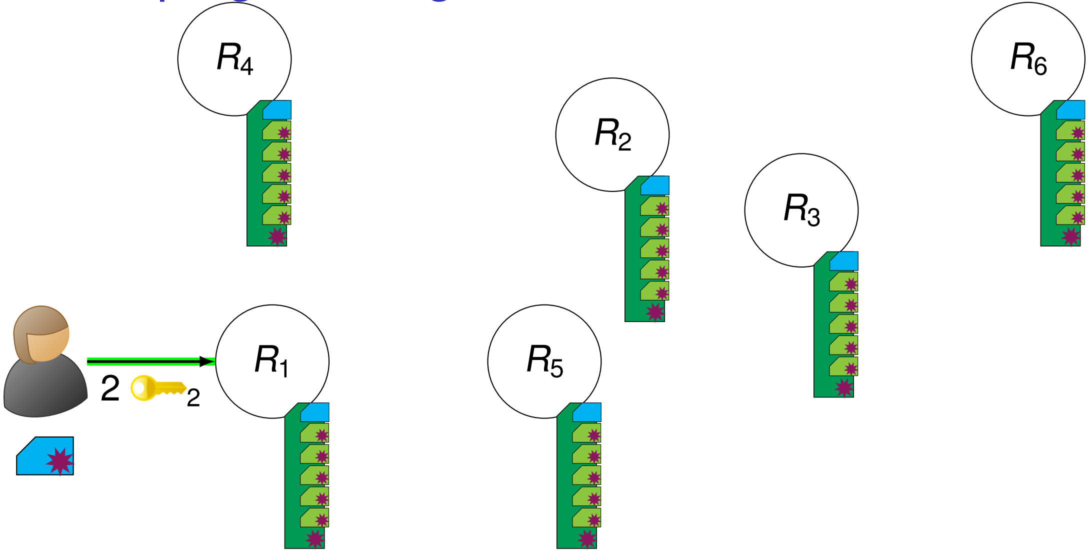
Telescoping Walking Onions



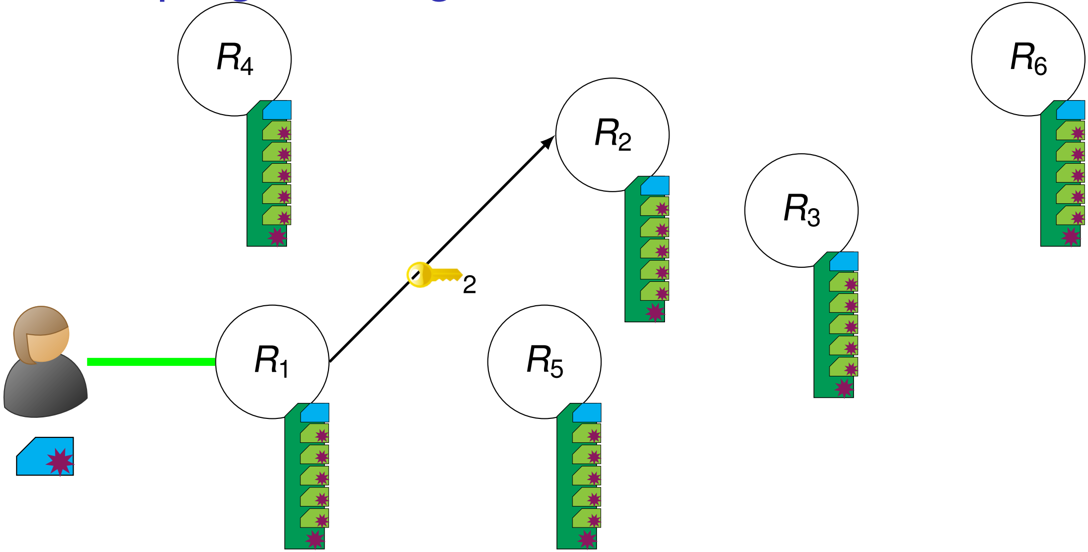
Telescoping Walking Onions



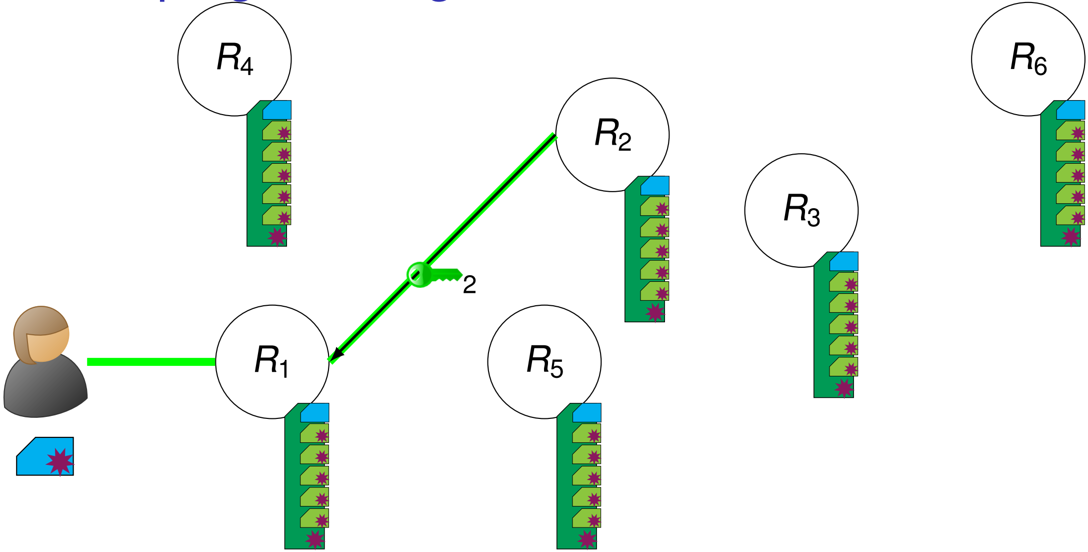
Telescoping Walking Onions



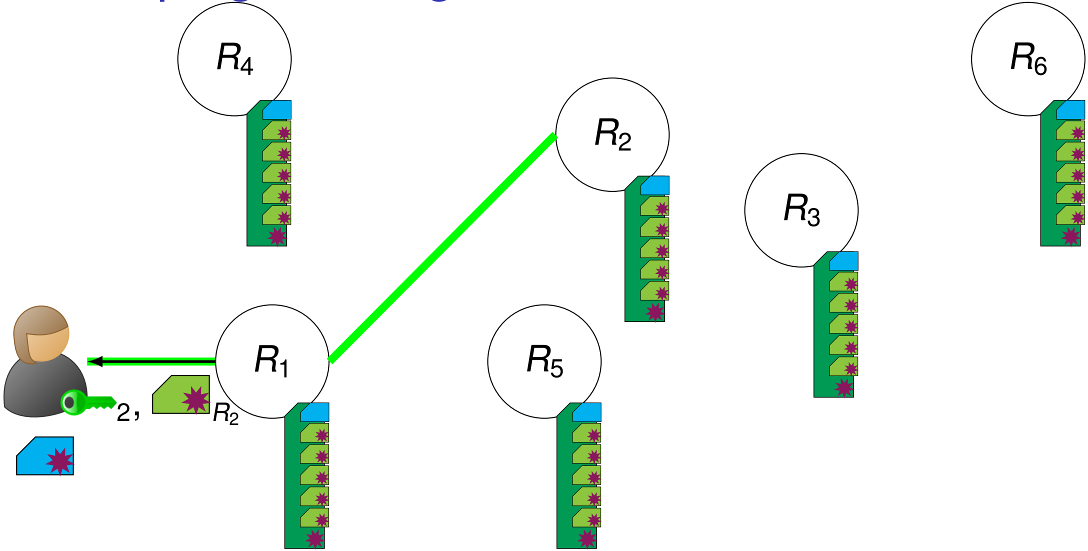
Telescoping Walking Onions



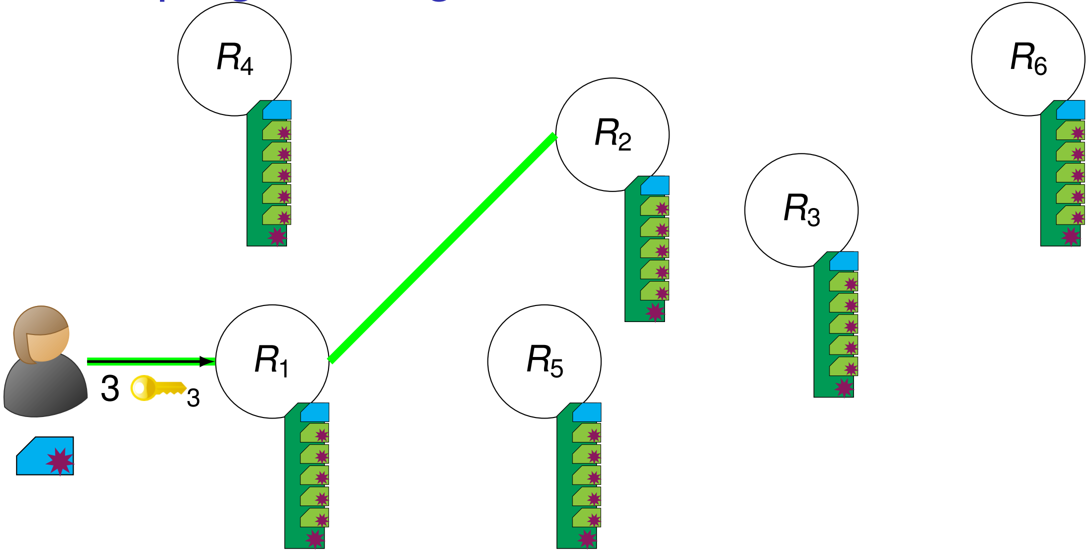
Telescoping Walking Onions



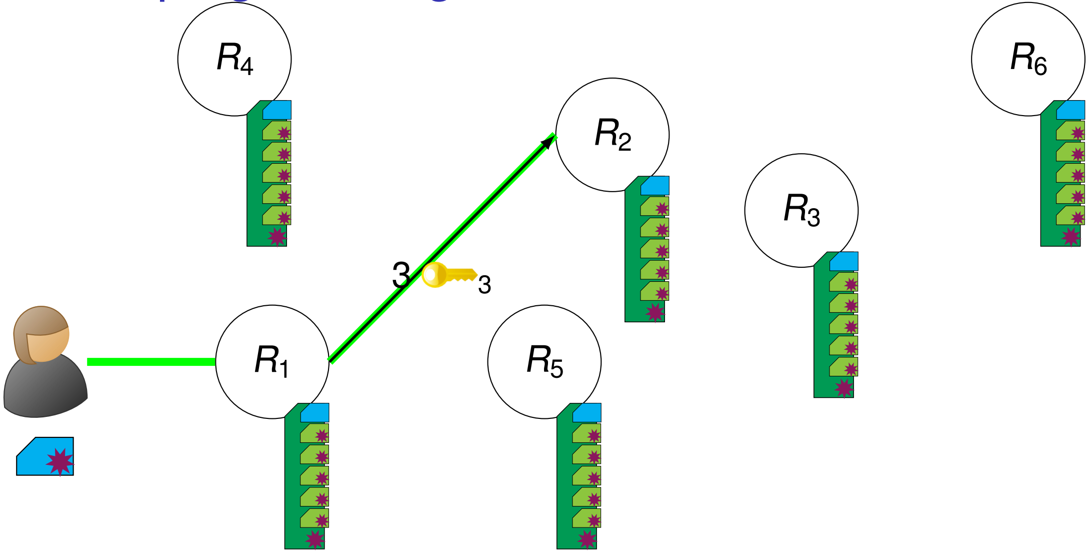
Telescoping Walking Onions



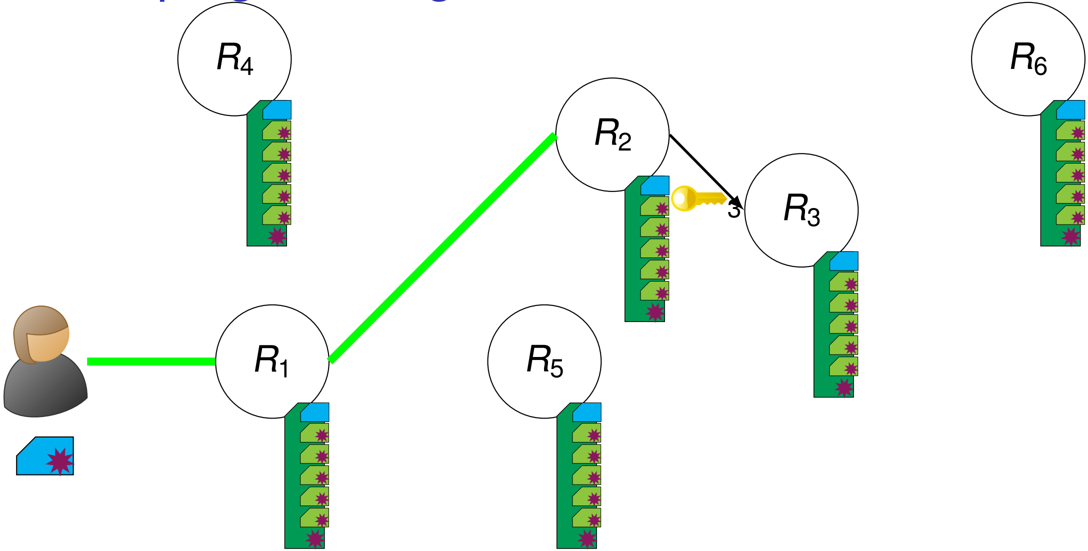
Telescoping Walking Onions



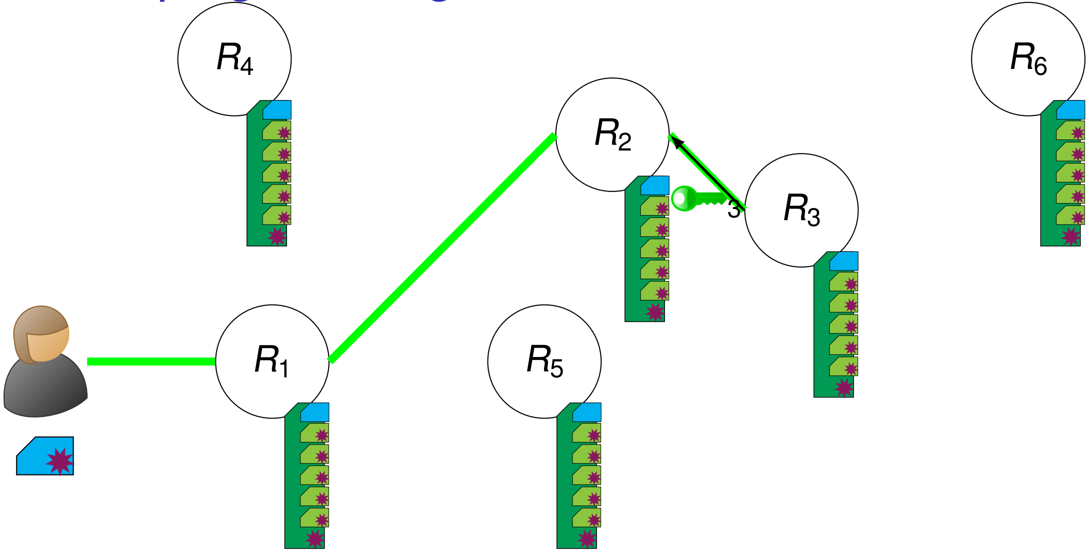
Telescoping Walking Onions



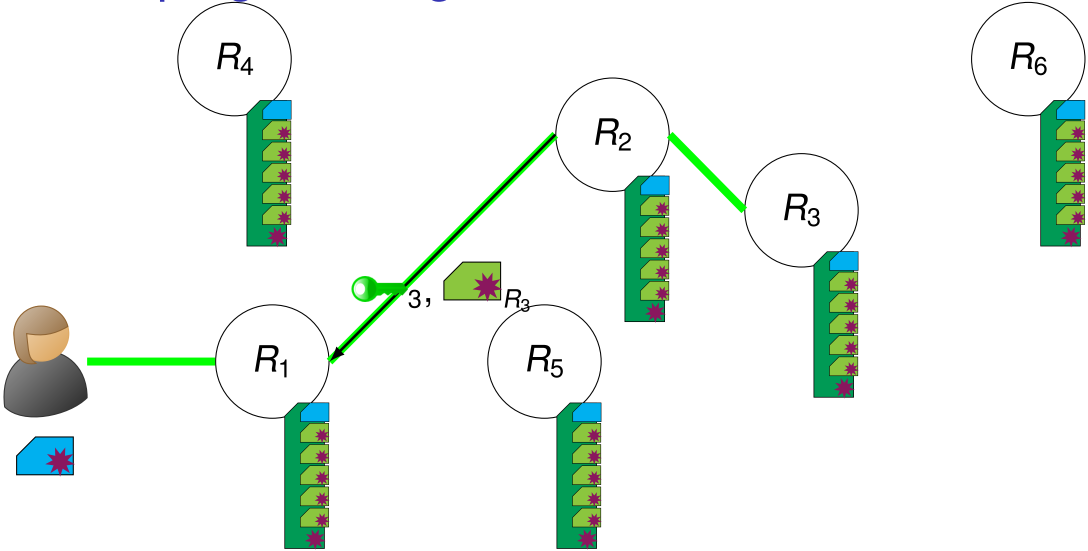
Telescoping Walking Onions



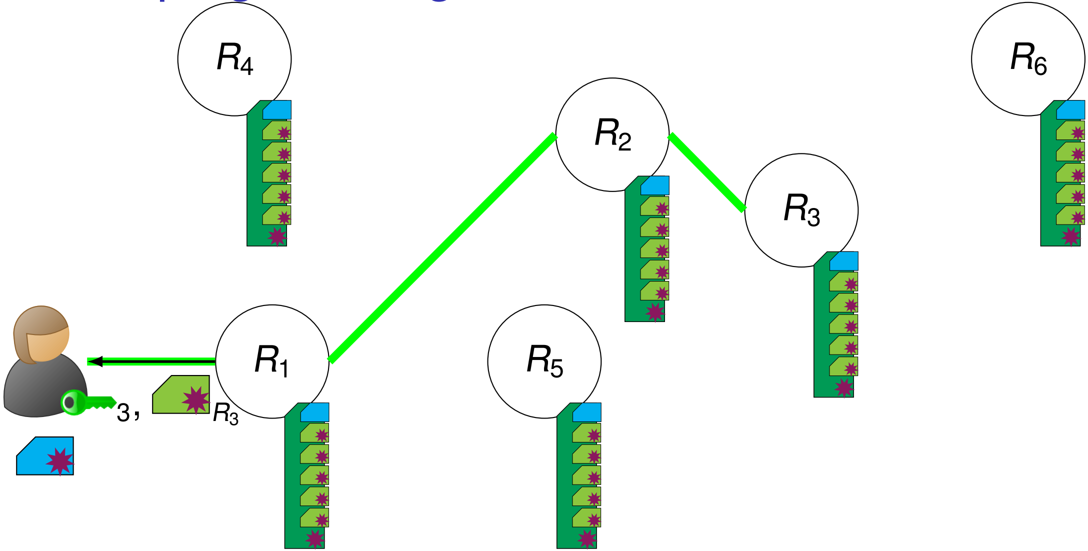
Telescoping Walking Onions



Telescoping Walking Onions



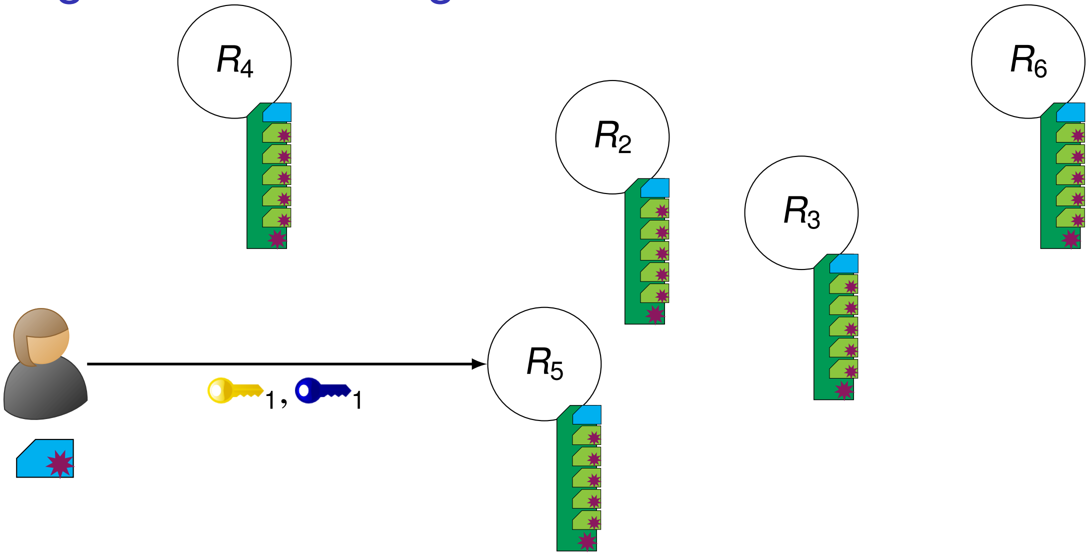
Telescoping Walking Onions



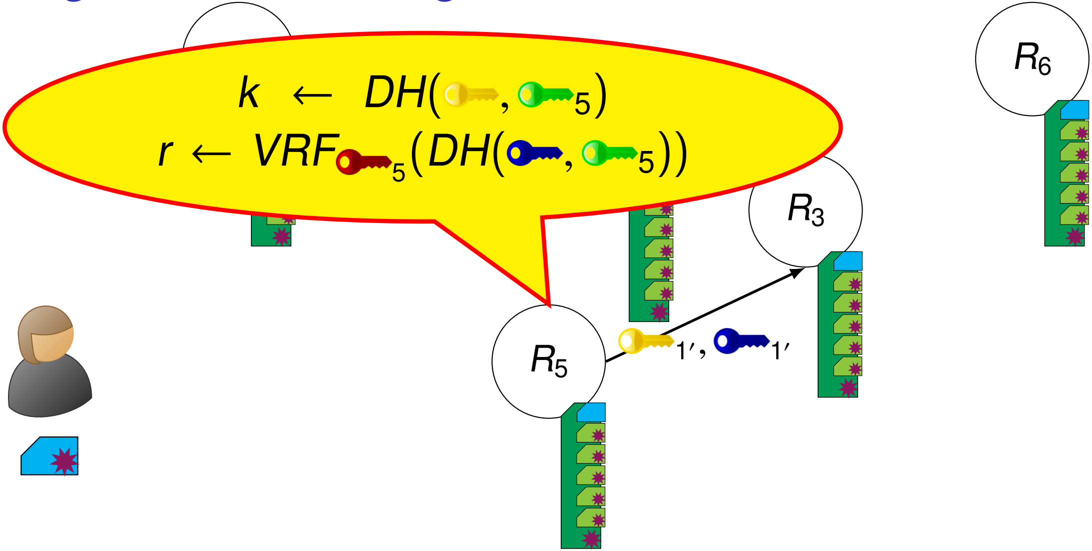
What improvements does Walking Onions make?

- How to represent relay information to enable oblivious selection and individual verification?
- How to build paths using oblivious relay selection?
- **How to perform more efficient circuit construction?**

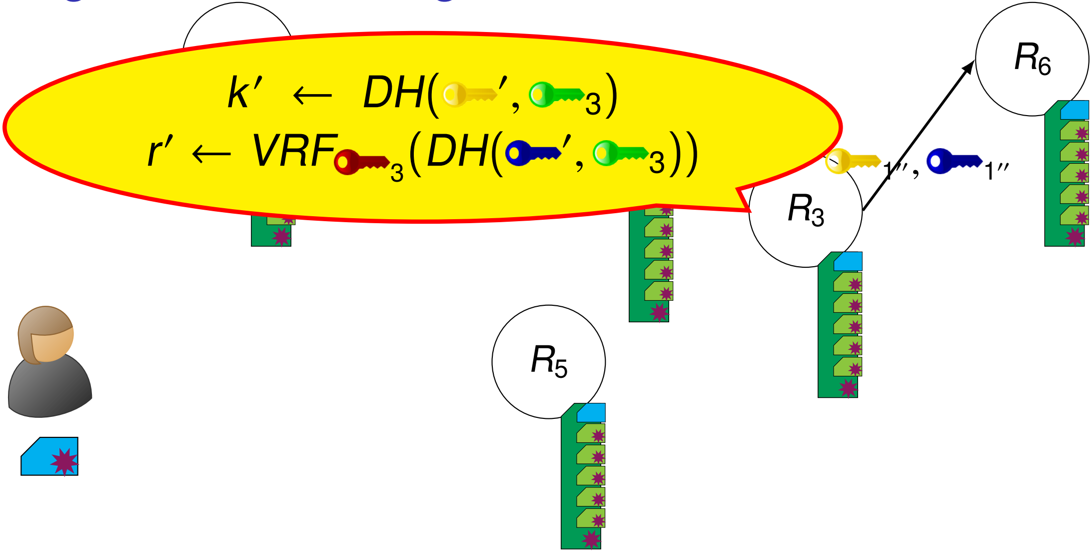
Single-Pass Walking Onions



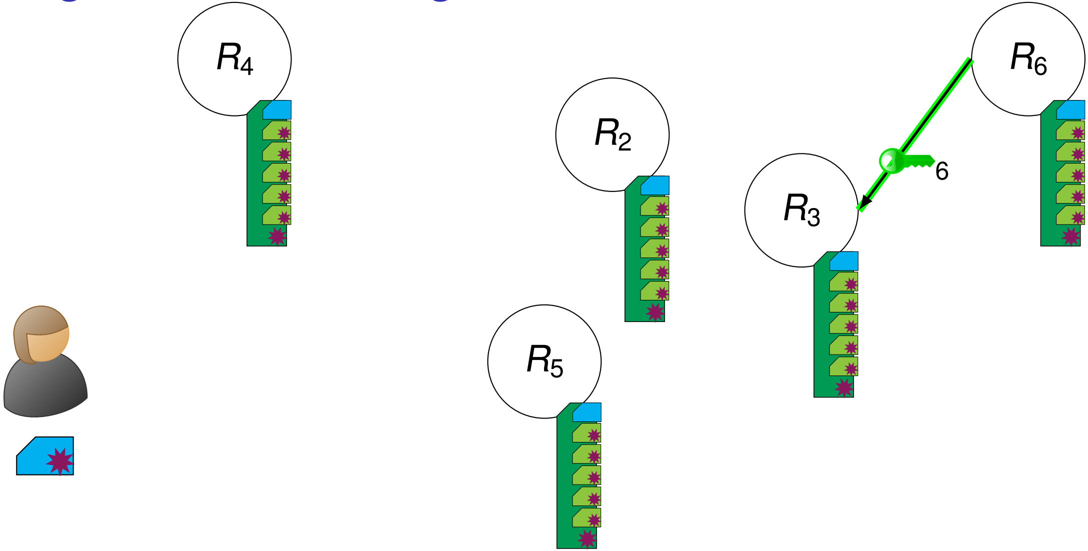
Single-Pass Walking Onions



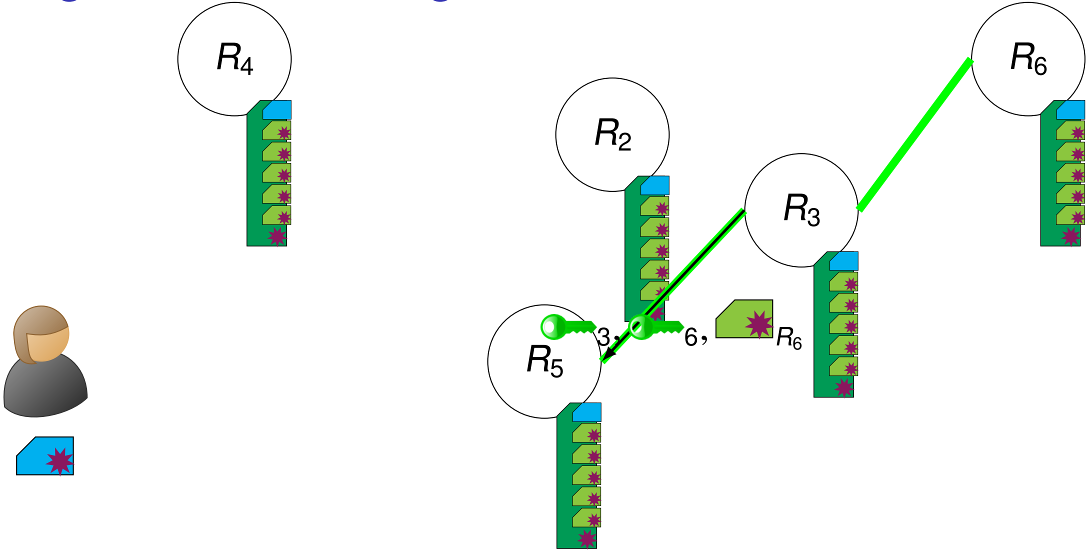
Single-Pass Walking Onions



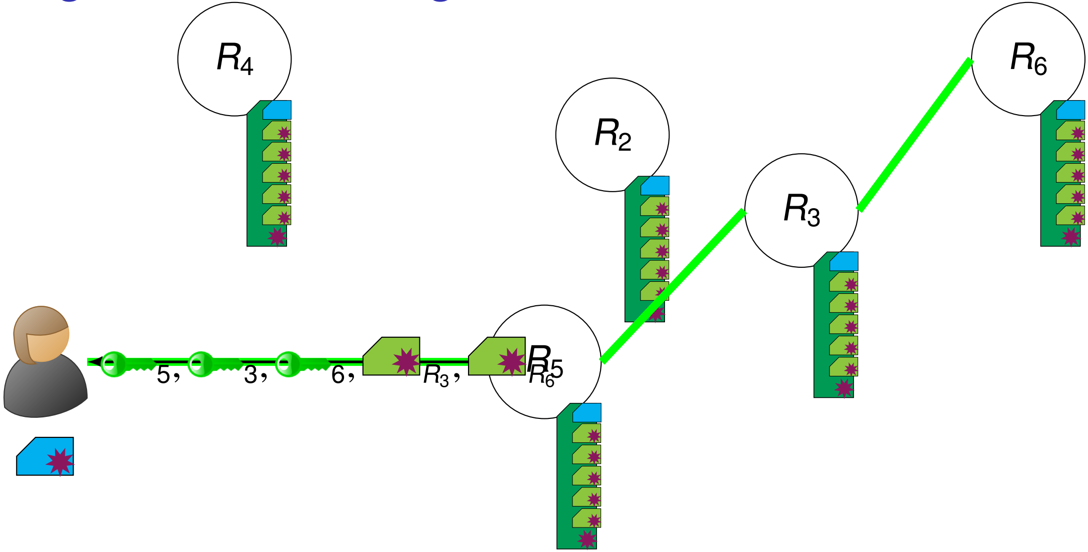
Single-Pass Walking Onions



Single-Pass Walking Onions

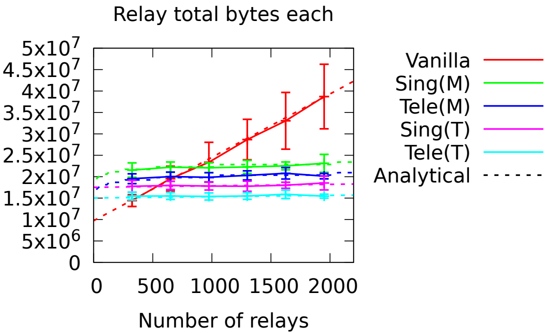


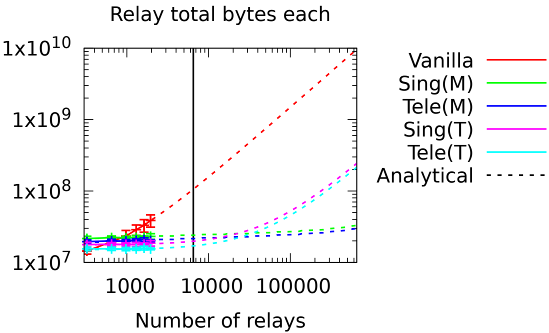
Single-Pass Walking Onions



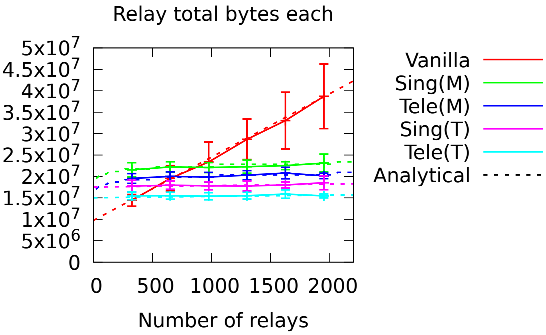
Performance Evaluation

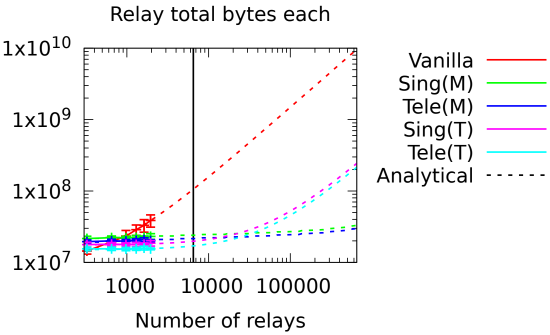
Bandwidth Results for Tor Relays





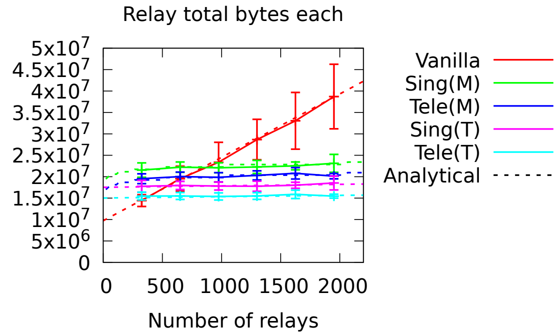
Bandwidth Results for Tor Relays

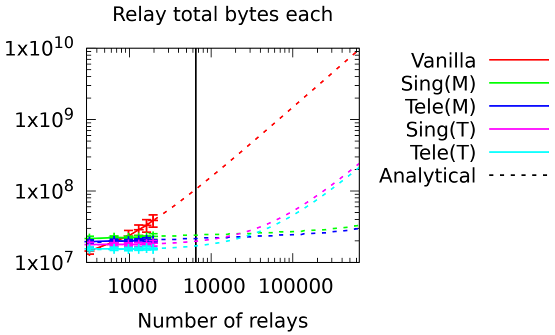




- Walking Onions requires 4–6 times less bandwidth than Vanilla Onion Routing at a network the size of Tor today.

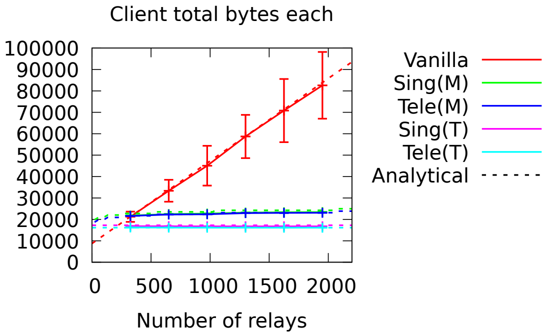
Bandwidth Results for Tor Relays

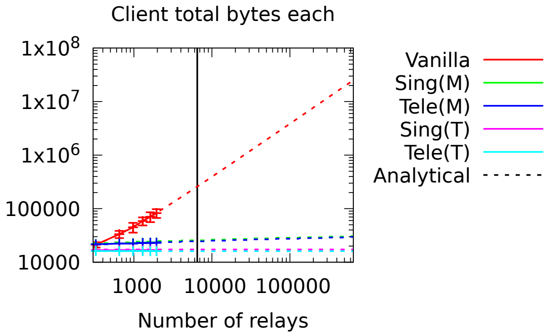




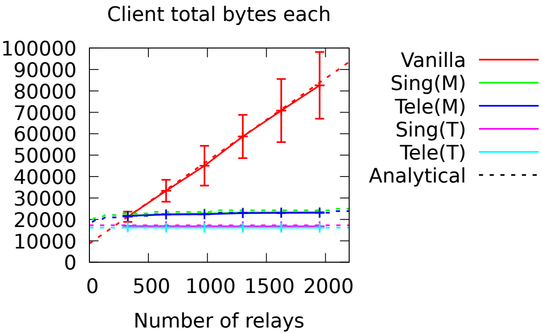
- Walking Onions requires 4–6 times less bandwidth than Vanilla Onion Routing at a network the size of Tor today.
- Improvement of 25–40 times less bandwidth at a network 10 times the size of Tor.

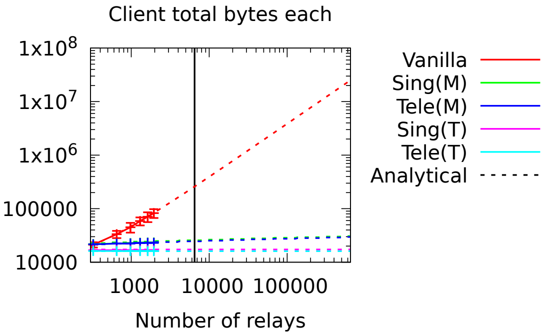
Bandwidth Results for Tor Clients





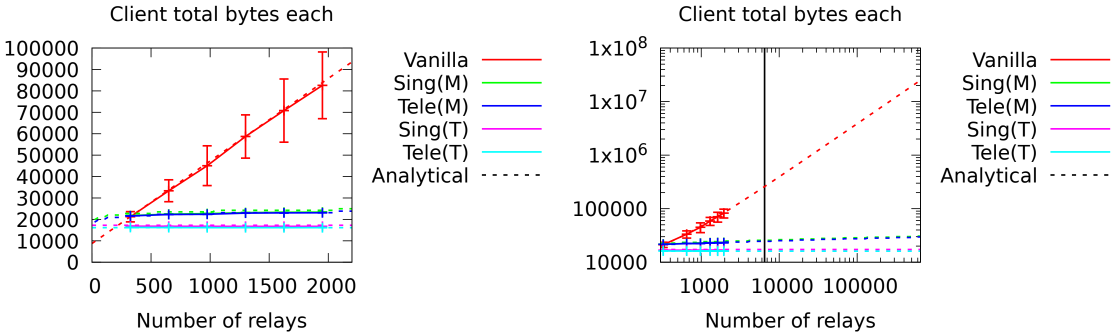
Bandwidth Results for Tor Clients





- Clients in Walking Onions save 10–15 times the bandwidth over Vanilla Onion Routing in a network the size of Tor today.

Bandwidth Results for Tor Clients



- Clients in Walking Onions save 10–15 times the bandwidth over Vanilla Onion Routing in a network the size of Tor today.
- In a network 10 times the size of Tor, Walking Onions saves clients 90–150 times the bandwidth over Vanilla.

Takeaways

- The design of Tor today imposes impractical overheads to clients as the network scales.

Find our paper and artifact at https://crysp.uwaterloo.ca/software/walkingonions

Takeaways

- The design of Tor today imposes impractical overheads to clients as the network scales.
- Walking Onions:

Find our paper and artifact at https://crysp.uwaterloo.ca/software/walkingonions

Takeaways

- The design of Tor today imposes impractical overheads to clients as the network scales.
- Walking Onions:
  - Removes the per-relay bandwidth and storage cost to clients

Find our paper and artifact at https://crysp.uwaterloo.ca/software/walkingonions

Takeaways

- The design of Tor today imposes impractical overheads to clients as the network scales.
- Walking Onions:
  - Removes the per-relay bandwidth and storage cost to clients
  - Offers the same security protections against epistemic and route capture attacks as prior designs that required a globally consistent view.

Find our paper and artifact at https://crysp.uwaterloo.ca/software/walkingonions

Takeaways

- The design of Tor today imposes impractical overheads to clients as the network scales.
- Walking Onions:
  - Removes the per-relay bandwidth and storage cost to clients
  - Offers the same security protections against epistemic and route capture attacks as prior designs that required a globally consistent view.
- Tor has already begun the specification work to integrate Walking Onions into the Tor protocol.

Find our paper and artifact at https://crysp.uwaterloo.ca/software/walkingonions