Mix Networks with Restricted Routes

George Danezis
University of Cambridge
Computer Laboratory

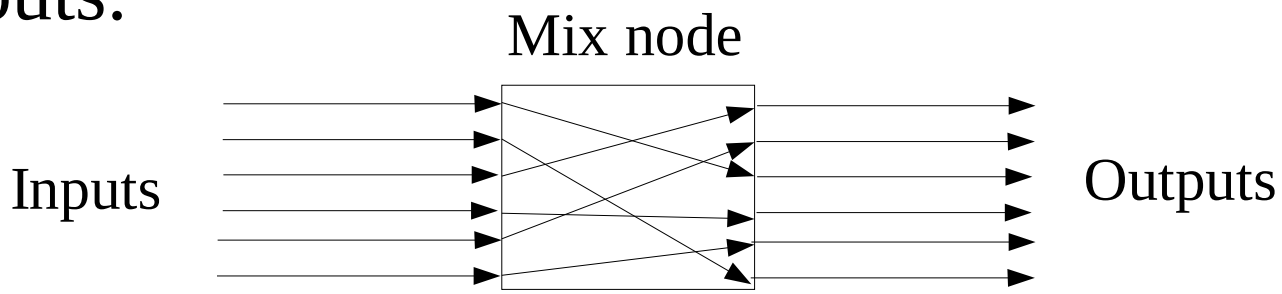
Privacy Enhancing Technologies Workshop 2003

Summary

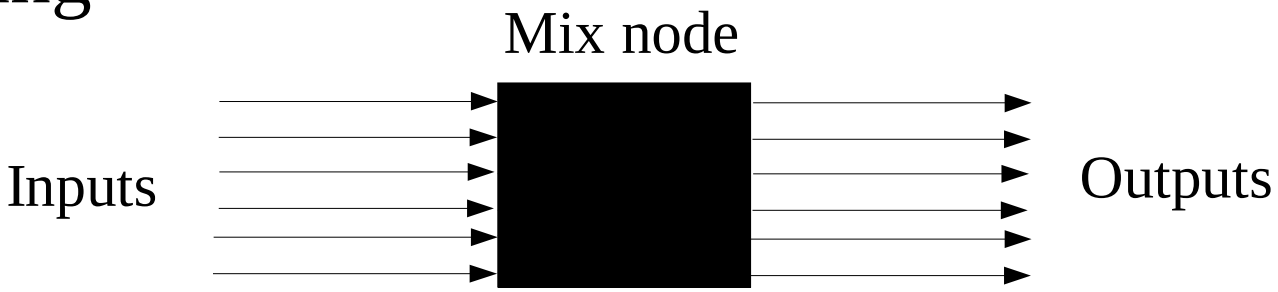
- 'Brief' introduction to mixes and mix networks
  - Basic building blocks and networks
- Abstracting mix networks as mixes
  - Assessing the anonymity they provide
- Properties
  - Resistance to traffic analysis, volumes of traffic...
- What about restricted routes?

Basic building block: **The MIX**

- Hiding correspondence between inputs and outputs.

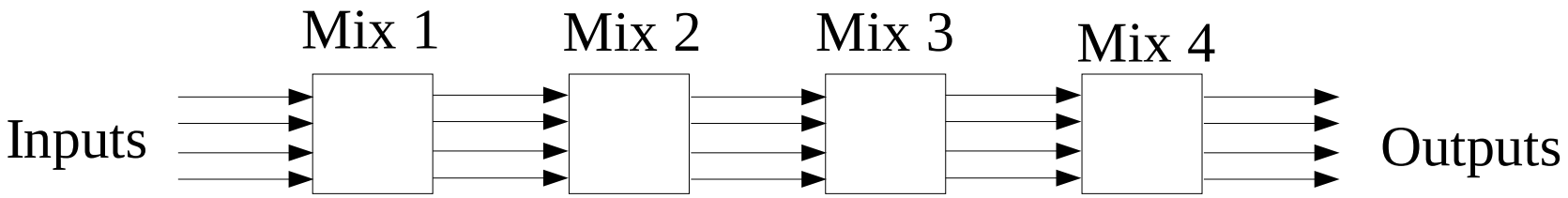


- An adversary's view: bitwise unlinkability + mixing



Distributing trust: Cascade

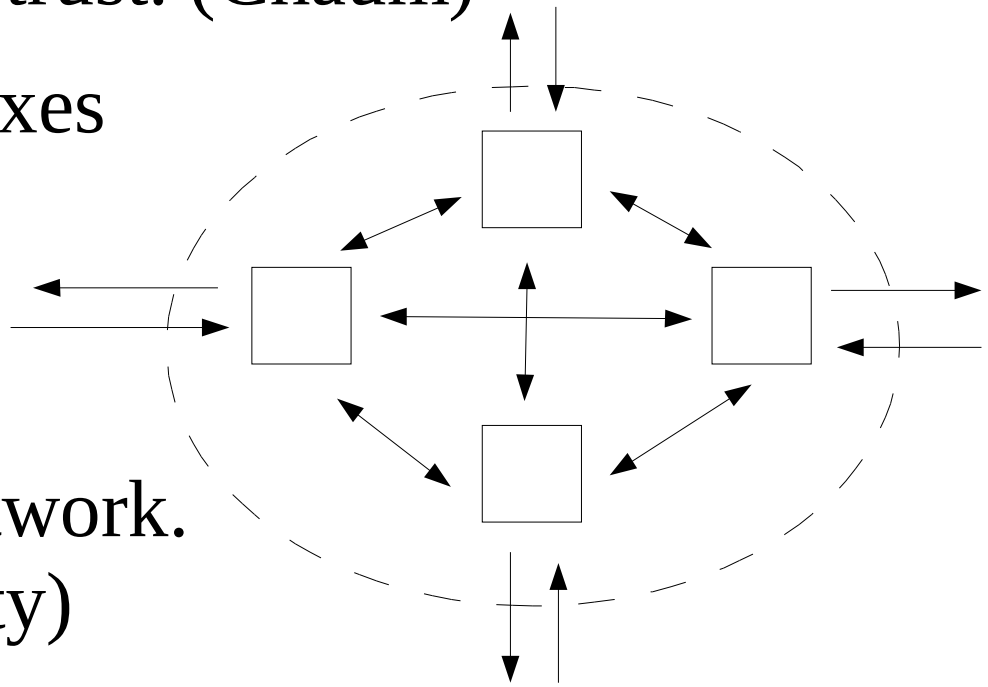
- If the mix is corrupt then there is no anonymity.
- Solution cascade of mixes (Berthold):



- If one mix is honest then we still have maximal anonymity.
- But: Latency is increased.

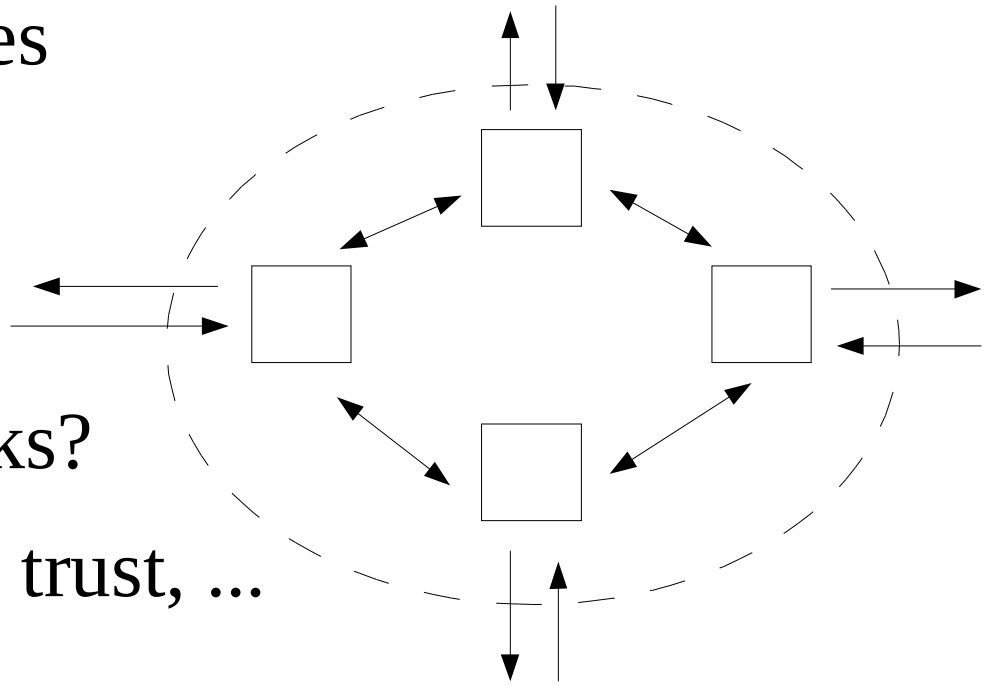
Distributing load: Mix Networks

- To decrease the latency, and distribute the load while still distributing trust. (Chaum)
- Original design: all mixes can talk to all others.
- Client needs to choose a route through the network. (sub-optimal anonymity)



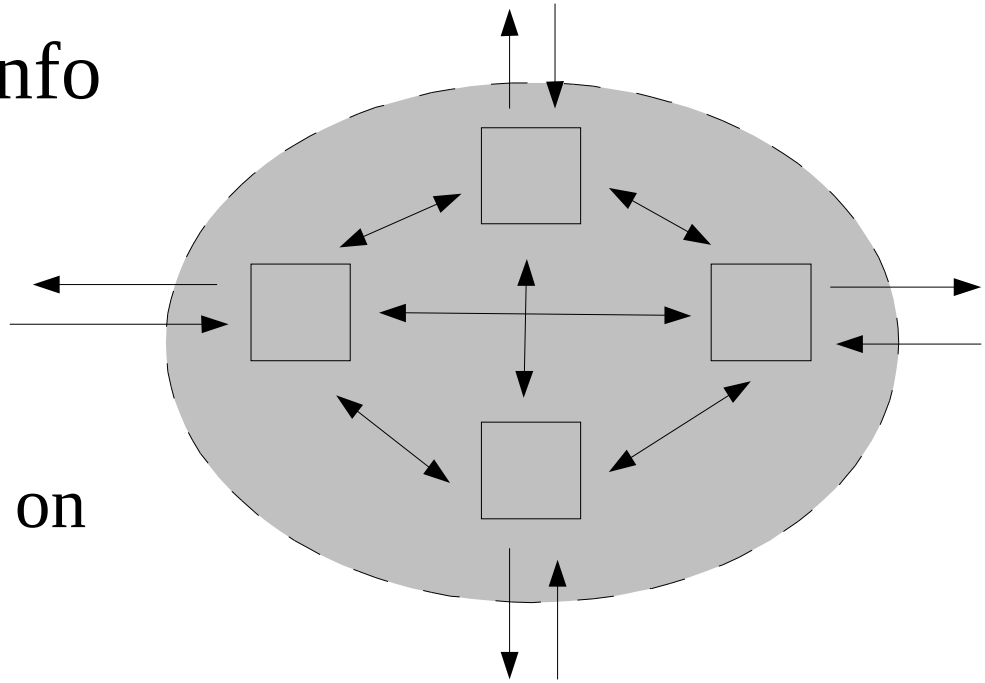
Mix network with restricted routes

- For some reason mixes can only talk to a few neighbors (topology, padding, bandwidth, ...)
- Route selection requires more information.
- How does this compares to fully connected mix networks?
- Other properties: DoS, trust, ...



Mix networks as abstract mixes

- What we would like the adversary to see is only the inputs and outputs. Perfect Mixing...
- But in practice other info is also available:
  - Topology
  - First and last mix
  - Traffic characteristics on each link.



Traffic Confirmation vs. Traffic Analysis

- Traffic confirmation (Syverson et al.):
  - Attacks that do not use the additional info leaked by the network.
  - Topology affects them but we will not discuss further...
- Traffic analysis:
  - Attacks that make use of the additional information. (Topology, route length, traffic characteristics, ...)
- 'Traffic analysis of restricted routes networks'.

Properties Required

- Anonymity defined in information theoretic terms (Serjantov, Danezis).
  - Route selection knowledge cannot reduce anonymity.
  - Uniform anonymity is provided.
  - The traffic observed should not give much additional information to attacker.
  - Resistance to intersection attacks (in network).
- Other: Resistance to corrupt nodes, active attacks, DoS.

Modeling Mix Networks

- We model mix networks using Graph Theory.
- The Route selection process is approximated by a random walk on the topology graph.
  - We require this to lead to the stationary prob. Dist. from any starting node (uniformity)
- The 'Traffic Matrix' describes the actual probabilities assigned to a message given the observed traffic in the network.
  - A random walk on this matrix should lead to the same distribution as the above.

Assessing the route length

- **Key result:** if the network has 'good mixing properties' only O(logN) steps are required.
  - The mixing is uniform in O(logN)
- Good mixing properties:
  - Topology is an Expander Graph.
  - Constant degree D graphs (each node only knows few neighbors) have such properties.
  - Gory detail: Exact number of rounds depends on the spectral gap between the first and second eigenvalue of graph.

How much traffic is required?

- The aim is to make:
  'traffic matrix' = topology matrix
- We can require it to only deviate by a small percentage on all links.
  - Assuming that the route selection was done using the topology matrix calculate after how much traffic they converge.
  - The choice of next link at each node is described by the multinomial dist: Calculate the volume requited to get the expectation (depends on mixing strategy).

Resistance to Intersection Attacks

- Intersection attacks on the mixes (Berthold).
  - Replay attacks or streams of messages using the same path.
- **Key result:** needs K>O(bp/(1-p)) rounds to confirm that a messages takes a path.
  - Where b is the batch size and p the prob of taking the link tested.
  - Result only valid for threshold mix.
- The smaller the number of links (as in restricted routes) the larged min(p) -> the larger K.

Advantages of Restricted Routes

- Quick mixing: in O(logN) steps.
- Better resistance to intersection attacks.
- Scale well: Only O(N) amount of traffic is required in the network at any time to make it secure against traffic analysis.
- Analysis of fully connected mix networks:
  - TM is not equal to route selection matrix in general.
  - Resistance to intersection attacks is poor.
  - Does not automatically mean they are broken!

Conclusions & Further directions

- A better understanding of general mix networks.
- Further work should look at resistance to corrupt nodes, denial of service attacks and active attacks.
- Results are dependent on a good expander graph topology. Who creates it? How is it managed?
- Resistance to intersection and TA attacks lead us to the topic of cover traffic.
- Less general restricted route topologies with more provable properties...

Questions?

- Contact details:
  http://www.cl.cam.ac.uk/~gd216
  George.Danezis@cl.cam.ac.uk