The Loopix Anonymity System

Ania M. Piotrowska\textsuperscript{1} Jamie Hayes\textsuperscript{1} Tariq Elahi\textsuperscript{2} Sebastian Meiser\textsuperscript{1} George Danezis\textsuperscript{1}

\textsuperscript{1}University College London, UK \hspace{1em} \textsuperscript{2}KU Leuven
Mixnets Background

A set of cryptographic relays hiding input and output correspondence, by using layered encryption and secret permutation.
Motivation

Mixnet design shortcomings:

In order to guarantee anonymity, mixnet requires long delays (high latency) and cover traffic (scalability).
Not resistant against active attacks.
No support for offline delivery.

Onion-routing design shortcomings:

Not resistant against global passive adversary.
Loopix Overview

A new mixnet-based anonymous communication system, allowing for a tunable trade-off between **latency** and **genuine and cover traffic** volume.
Loopix Overview

A new mixnet-based anonymous communication system, allowing for a tunable trade-off between latency and genuine and cover traffic volume.
End-to-end messages
Drop cover traffic
Client’s loop cover traffic
Mix’s loop cover traffic
Client - Provider Link

**Sending** - each stream of traffic follows a Poisson process

\[ \Lambda_P + \Lambda_D + \Lambda_L \]

**Retrieving** - a fixed number of packets from the Provider
Mixing strategy - Poisson mix

Each packet is delayed according to a sender determined exponential delay.

Properties:

Poisson mix can be modeled as a pool mix.

Messages in the mix pool are indistinguishable due to the memoryless property.

No synchronized rounds required.
## Security Properties - Summary

<table>
<thead>
<tr>
<th>Property</th>
<th>GPA</th>
<th>Corrupt mixes</th>
<th>Corrupt provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender-Recipient Third-Party Unobservability</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sender online unobservability</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sender anonymity</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Receiver unobservability</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Receiver anonymity</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>
Anonymity vs Latency vs Rate of traffic

**Figure:** Entropy versus the changing rate of the incoming traffic for different delays (seconds). Lower $\mu$ is a higher delay.
Performance - Throughput

Figure: Overall bandwidth and goodput per second for a single mix node.

Starting conditions:

- $\Lambda_P = 3 \text{ msg/min}$
- $\Lambda_L = 1 \text{ msg/min}$
- $\Lambda_D = 1 \text{ msg/min}$
- $\Lambda_M = 1 \text{ loop/min}$
- Avg. delay / hop = 1 ms

Periodic increase by 2 msg/min
Performance - Latency Overhead

\[ \Lambda = 30 \text{ msg/min} \]

\[ \Lambda_M = 10 \text{ loops/min} \]
Performance - End-to-end Message Latency

Figure: End-to-end latency histogram.

\[ \Lambda = 180 \text{ msg/min} \]

\[ \Lambda_M = 60 \text{ loops/min} \]

Avg. delay / hop
= 0.5 sec
Loopix Key takeaways

Unlinkability of senders and recipients
Detection of active attacks
Unobservability of clients actions
Balanced trade-off between latency and cover traffic
Supporting off-line storage
Loopix Key takeaways

Unlinkability of senders and recipients
Detection of active attacks
Unobservability of clients actions
Balanced trade-off between latency and cover traffic
Supporting off-line storage

Loopix Implementation: https://github.com/UCL-InfoSec/loopix
My Website: http://www0.cs.ucl.ac.uk/staff/A.Piotrowska/
My E-mail: a.piotrowska@cs.ucl.ac.uk

Thank you!
<table>
<thead>
<tr>
<th></th>
<th>Low Latency</th>
<th>Low Communication Overhead</th>
<th>Scalable Deployment</th>
<th>Asynchronous Messaging†</th>
<th>Active Attack Resistant</th>
<th>Offline Storage*</th>
<th>Resistance to GPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopix</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Dissent</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Vuvuzela</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Stadium</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Riposte</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Atom</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Riffle</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>AnonPoP</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Tor</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>

**Table:** Comparison of popular anonymous communication systems. By *, we mean if the design intentionally incorporates provisions for delivery of messages when a user is offline, perhaps for a long period of time. By †, we mean that the system operates continuously and does not depend on synchronized rounds for its security properties and users do not need to coordinate to communicate together.